Benutzerhandbuch

Real-Time-Ethernet-Kit

Analysebeispiele

Hilscher Gesellschaft für Systemautomation mbH

www.hilscher.com

DOC081202UM04DE | Revision 4 | Deutsch | 2012-11 | Freigegeben | Öffentlich

Inhaltsverzeichnis

1 EINLEITUNG 4
1.1 Über das Benutzerhandbuch 4
1.1.1 Änderungsübersicht 4
1.1.2 Konventionen in diesem Handbuch 5
1.1.3 Weitere Informationen 6
1.2 Rechtliche Hinweise 7
1.2.1 Copyright 7
1.2.2 Wichtige Hinweise 7
1.2.3 Haftungsausschluss 8
1.2.4 Gewährleistung 8
1.2.5 Exportbestimmungen 9

2 MEßMETHODEN UND BEISPIELE 10
2.1 Meßmethoden 10
2.2 Übersicht der Messbeispiele 10

3 VORAUSSETZUNGEN ZUR DURCHFÜHRUNG DER MESSUNGEN 11
3.1 Hardware und Software Installation 11
3.2 Aufzeichnung der Datentelegramme 11
3.3 netANALYZER einrichten 12
3.3.1 Einstellungen für die Telegrammaufzeichnung 13
3.4 Skalierungen im Timing-Analyse Fenster 14
3.4.1 Skalierung mit den Schiebereglern 14
3.4.2 Skalierung mit der Maus 15

4 PROFINET IO ANALYSE 16
4.1 Hardware-Aufbau 16
4.2 Zeitmessungen vorbereiten und durchführen 17
4.2.1 Zeitmessung vorbereiten 17
4.2.2 Filter einstellen 18
4.2.3 Signalflussrichtung ermitteln 22
4.2.4 Einstellungen in den Analysefenstern 24
4.2.5 Messung durchführen 25
4.3 Datenaufzeichnungen durchführen 28
4.4 Netzlast-Analyse vorbereiten und durchführen 34
4.4.1 Netzlast-Analyse vorbereiten 34
4.4.2 Filter einstellen 35
4.4.3 Netzlast-Messung durchführen 39

5 ETHERCAT ANALYSE 42
5.1 Hardware-Aufbau 42
5.2 Zeitmessungen vorbereiten und durchführen 43
5.2.1 Zeitmessung vorbereiten 43
5.2.2 Filter einstellen 44
5.2.3 Einstellungen in den Timing-Analysefenstern 45
5.2.4 Messung durchführen 47

© Hilscher, 2008-2012

5.3 Datenaufzeichnungen durchführen 53

6 ETHERNET/IP ANALYSE 58
6.1 Hardware-Aufbau 58
6.2 Datenaufzeichnung durchführen 59
6.2.1 Verbindungs-ID ermitteln 63
6.3 Zeitmessung vorbereiten und durchführen 64
6.3.1 Zeitmessung vorbereiten 64
6.3.2 Filter einstellen 66
6.3.3 Einstellungen in den Timing-Analysefenstern 70
6.3.4 Messungen durchführen 71
6.4 Datenaufzeichnungen durchführen 76
6.5 Netzlast-Analyse vorbereiten und durchführen 80
6.5.1 Netzlast-Analyse vorbereiten 80
6.5.2 Filter einstellen 80
6.5.3 Netzlast-Messung durchführen 84

7 SERCOS ANALYSE 87
7.1 Hardware-Aufbau 87
7.2 Zeitmessung vorbereiten und durchführen 88
7.2.1 Zeitmessung vorbereiten 88
7.2.2 Filter einstellen 89
7.2.3 Einstellungen in den Timing-Analysefenstern 91
7.2.4 Messung durchführen 93
7.3 Datenaufzeichnungen durchführen 98

8 MODBUS/TCP ANALYSE 102
8.1 Hardware-Aufbau 102
8.2 Zeitmessung vorbereiten und durchführen 103
8.2.1 Zeitmessung vorbereiten 103
8.2.2 Filter einstellen 104
8.2.3 Einstellungen in den Timing-Analysefenstern 109
8.2.4 Messungen durchführen 111
8.3 Datenaufzeichnung durchführen 116
8.4 Netzlast-Analyse vorbereiten und durchführen 120
8.4.1 Netzlast-Analyse vorbereiten 120
8.4.2 Filter einstellen 120
8.4.3 Netzlastmessung durchführen 124

9 GLOSSAR 127

10 ANHANG 128
10.1 Abbildungsverzeichnis 128
10.2 Tabellenverzeichnis 130
10.3 Kontakte 131

© Hilscher, 2008-2012

1 Einleitung

1.1 Über das Benutzerhandbuch

Dieses Benutzerhandbuch enthält Beschreibungen von Messbeispielen, die mit den Komponenten des Real-Time-Ethernet-Kit's aufgebaut werden können.

1.1.1 Änderungsübersicht

Index	Datum	Hard- / Software	Kapitel	Änderungen
1	11.12.08	Real-Time-Ethernet-Kit	alle	Erstellt
2	10.03.09	Real-Time-Ethernet-Kit		Anpassung an netANALYZER, Softwareversion 1.2.0.0
3	01.07.10	Real-Time-Ethernet-Kit	alle	Anpassung an netANALYZER, Softwareversion 1.3.0.0 an CIFX 50-RE Rev. 3
4	19.11.12	Real-Time-Ethernet-Kit	alle	Anpassung an netANALYZER, Softwareversion 1.4.x.x Neue Funktionen: Netzlast-Analyse (Netload Analysis), History-Darstellung

Tabelle 1: Änderungsübersicht

© Hilscher, 2008-2012

1.1.2 Konventionen in diesem Handbuch

Handlungsanweisungen, ein Ergebnis eines Handlungsschrittes bzw. Hinweise sind wie folgt gekennzeichnet:

Handlungsanweisungen:

➢ <Anweisung>

oder

1. <Anweisung>
2. <Anweisung>

Ergebnisse:

⇘ <Ergebnis>

Hinweise:

Wichtig: <Wichtiger Hinweis>

Hinweis: <Hinweis>

<Hinweis, wo Sie weitere Informationen finden können>

Positionen im Bild

Die *Positionen* ①, ②, ③ **...** oder ⓐ, ⓑ, ⓒ **...** oder Ⓐ, Ⓑ, Ⓒ **...** beziehen sich auf die in dem Abschnitt verwendete Abbildung. Dies ist in der Regel die Abbildung, die unmittelbar oberhalb des Textes platziert ist. Wenn sich die Positionen im Bild auf eine Abbildung außerhalb des Abschnitts beziehen, ist auf diesen Abschnitt speziell verwiesen.

© Hilscher, 2008-2012

1.1.3 Weitere Informationen

In diesem Dokument wird auf die Benutzerhandbücher der einzelnen Komponenten

netANALYZER-Karte PCI RTE - NANL-C500-RE,

netANALYZER-Box PCIe RTE - NANL-B500E-RE,

und netANALYZER-Software, SW Version 1.4.

cifX-Karten Real-Time-Ethernet

NXIO 50-RE-Board

sowie dem Benutzerhandbuch Real-Time-Ethernet Kit Installation, Bedienung und Konfiguration

verwiesen.

Hinweis: Die Zusammenschaltung der NXIO 50-RE Boards, wie in den Messbeispielen dargestellt, ist nur unter Laborbedingungen zulässig.

Hinweis: Beachten Sie die Hinweise zur Wireshark Installation im Benutzerhandbuch netANALYZER Rev. 12 Abschnitt 14.3.

© Hilscher, 2008-2012

1.2 Rechtliche Hinweise

1.2.1 Copyright

© Hilscher, 2008-2012, Hilscher Gesellschaft für Systemautomation mbH

Alle Rechte vorbehalten.

Die Bilder, Fotografien und Texte der Begleitmaterialien (Benutzerhandbuch, Begleittexte, Dokumentation etc.) sind durch deutsches und internationales Urheberrecht sowie internationale Handels- und Schutzbestimmungen geschützt. Sie sind ohne vorherige schriftliche Genehmigung nicht berechtigt, diese vollständig oder teilweise durch technische oder mechanische Verfahren zu vervielfältigen (Druck, Fotokopie oder anderes Verfahren), unter Verwendung elektronischer Systeme zu verarbeiten oder zu übertragen. Es ist Ihnen untersagt, Veränderungen an Copyrightvermerken, Kennzeichen, Markenzeichen oder Eigentumsangaben vorzunehmen. Darstellungen werden ohne Rücksicht auf die Patentlage mitgeteilt. Die in diesem Dokument enthaltenen Firmennamen und Produktbezeichnungen sind möglicherweise Marken bzw. Warenzeichen der jeweiligen Inhaber und können warenzeichen-, marken- oder patentrechtlich geschützt sein. Jede Form der weiteren Nutzung bedarf der ausdrücklichen Genehmigung durch den jeweiligen Inhaber der Rechte.

1.2.2 Wichtige Hinweise

Das Benutzerhandbuch, Begleittexte und die Dokumentation wurden mit größter Sorgfalt erarbeitet. Fehler können jedoch nicht ausgeschlossen werden. Eine Garantie, die juristische Verantwortung für fehlerhafte Angaben oder irgendeine Haftung kann daher nicht übernommen werden. Sie werden darauf hingewiesen, dass Beschreibungen in dem Benutzerhandbuch, den Begleittexte und der Dokumentation weder eine Garantie, noch eine Angabe über die nach dem Vertrag vorausgesetzte Verwendung oder eine zugesicherte Eigenschaft darstellen. Es kann nicht ausgeschlossen werden, dass das Benutzerhandbuch, die Begleittexte und die Dokumentation nicht vollständig mit den beschriebenen Eigenschaften, Normen oder sonstigen Daten der gelieferten Produkte übereinstimmen. Eine Gewähr oder Garantie bezüglich der Richtigkeit oder Genauigkeit der Informationen wird nicht übernommen.

Wir behalten uns das Recht vor, unsere Produkte und deren Spezifikation, sowie zugehörige Benutzerhandbücher, Begleittexte und Dokumentationen jederzeit und ohne Vorankündigung zu ändern, ohne zur Anzeige der Änderung verpflichtet zu sein. Änderungen werden in zukünftigen Manuals berücksichtigt und stellen keine Verpflichtung dar; insbesondere besteht kein Anspruch auf Überarbeitung gelieferter Dokumente. Es gilt jeweils das Manual, das mit dem Produkt ausgeliefert wird.

Die Hilscher Gesellschaft für Systemautomation mbH haftet unter keinen Umständen für direkte, indirekte, Neben- oder Folgeschäden oder Einkommensverluste, die aus der Verwendung der hier enthaltenen Informationen entstehen.

1.2.3 Haftungsausschluss

Die Software wurde von der Hilscher Gesellschaft für Systemautomation mbH sorgfältig erstellt und getestet und wird im reinen Ist-Zustand zur Verfügung gestellt. Es kann keine Gewährleistung für die Leistungsfähigkeit und Fehlerfreiheit der Software für alle Anwendungsbedingungen und -fälle und die erzielten Arbeitsergebnisse bei Verwendung der Software durch den Benutzer übernommen werden. Die Haftung für etwaige Schäden, die durch die Verwendung der Hard- und Software oder der zugehörigen Dokumente entstanden sein könnten, beschränkt sich auf den Fall des Vorsatzes oder der grob fahrlässigen Verletzung wesentlicher Vertragspflichten. Der Schadensersatzanspruch für die Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen vorhersehbaren Schaden begrenzt.

Es ist strikt untersagt, die Software in folgenden Bereichen zu verwenden:

- für militärische Zwecke oder in Waffensystemen;
- zum Entwurf, zur Konstruktion, Wartung oder zum Betrieb von Nuklearanlagen;
- in Flugsicherungssystemen, Flugverkehrs- oder Flugkommunikationssystemen;
- in Lebenserhaltungssystemen;
- in Systemen, in denen Fehlfunktionen der Software körperliche Schäden oder Verletzungen mit Todesfolge nach sich ziehen können.

Sie werden darauf hingewiesen, dass die Software nicht für die Verwendung in Gefahrumgebungen erstellt worden ist, die ausfallsichere Kontrollmechanismen erfordern. Die Benutzung der Software in einer solchen Umgebung geschieht auf eigene Gefahr; jede Haftung für Schäden oder Verluste aufgrund unerlaubter Benutzung ist ausgeschlossen.

1.2.4 Gewährleistung

Obwohl die Hard- und Software mit aller Sorgfalt entwickelt und intensiv getestet wurde, übernimmt die Hilscher Gesellschaft für Systemautomation mbH keine Garantie für die Eignung für irgendeinen Zweck, der nicht schriftlich bestätigt wurde. Es kann nicht gewährleistet werden, dass die Hard- und Software Ihren Anforderungen entspricht, die Verwendung der Software unterbrechungsfrei und die Software fehlerfrei ist. Eine Garantie auf Nichtübertretung, Nichtverletzung von Patenten, Eigentumsrecht oder Freiheit von Einwirkungen Dritter wird nicht gewährt. Weitere Garantien oder Zusicherungen hinsichtlich Marktgängigkeit, Rechtsmängelfreiheit, Integrierung oder Brauchbarkeit für bestimmte Zwecke werden nicht gewährt, es sei denn, diese sind nach geltendem Recht vorgeschrieben und können nicht eingeschränkt werden. Gewährleistungsansprüche beschränken sich auf das Recht, Nachbesserung zu verlangen.

© Hilscher, 2008-2012

1.2.5 Exportbestimmungen

Das gelieferte Produkt (einschließlich der technischen Daten) unterliegt den gesetzlichen Export- bzw. Importgesetzen sowie damit verbundenen Vorschriften verschiedener Länder, insbesondere denen von Deutschland und den USA. Die Software darf nicht in Länder exportiert werden, in denen dies durch das US-amerikanische Exportkontrollgesetz und dessen ergänzender Bestimmungen verboten ist. Sie verpflichten sich, die Vorschriften strikt zu befolgen und in eigener Verantwortung einzuhalten. Sie werden darauf hingewiesen, dass Sie zum Export, zur Wiederausfuhr oder zum Import des Produktes unter Umständen staatlicher Genehmigungen bedürfen.

© Hilscher, 2008-2012

2 Meßmethoden und Beispiele

2.1 Meßmethoden

Alle Meßmethoden haben eine Auflösung von 10 ns. Der Messstart und die Messdauer kann durch externe Signale gesteuert werden.

Datenaufzeichnung

Mit der Datenaufzeichnung ist es möglich jedes Telegramm auf in einem Netzwerksegment in eine Datei zu speichern. Dabei können die Telegramme nach bestimmten Kriterien selektiert werden.

Zeitmessungen

Mit der Zeitmessung ist es möglich festzustellen wann welche Telegramme wie häufig im Netzwerk auftreten bzw. wie lange die Telegramme im Netzwerk zwischen zwei Punkten unterwegs sind.

Netzlast-Analyse

Mit der Netzlast-Analyse ist es möglich die Netzlast verschiedener über die Ethernet Leitung übertragener Protokolle zu messen. Dabei wird ersichtlich, welche Telegrammtypen zu welcher Zeit mit welcher Netzlast auftreten. Mit Hilfe der Netzlast-Analyse können auf diese Weise außergewöhnliche Ereignisse sichtbar gemacht werden.

Um hier keine Fehlmessungen zu erhalten, achten Sie darauf, dass Sie nur einen Port für die Messung aktivieren, um Doppelmessungen zu vermeiden.

2.2 Übersicht der Messbeispiele

Protokoll	Messtyp	Messung
PROFINET IO	Zeitmessung mit Hardware Filter	Zykluszeit, Telegramm-Durchlaufzeit durch einen IO Device.
	Telegrammaufzeichnung	Telegrammspeicherung mit Filter, Datenkonvertierung für Wireshark.
	Netzlast	PROFINET-Anlauf mit Filter auf bestimmte PROFINET-Telegramme.
EtherCAT	Zeitmessung mit Hardware Filter	Zykluszeit, Telegramm-Durchlaufzeit durch einen Slave und Ringdurchlaufzeit.
	Telegrammaufzeichnung	Telegrammspeicherung mit Datenkonvertierung für Wireshark.
EtherNet/IP	Zeitmessung mit Hardware Filter	Zykluszeit Master, Zykluszeit Slave, Durchlaufzeit Master Telegramme, Durchlaufzeit Slave Telegramme.
	Telegrammaufzeichnung	Telegrammspeicherung mit Datenkonvertierung für Wireshark.
	Netzlast	EtherNet/IP-Anlauf, Ping als Störung auf dem Netzwerk.
sercos	Zeitmessung mit Hardware Filter	Die Ringdurchlaufzeit des Primärrings, ConClk-Zykluszeit am Slave.
	Telegrammaufzeichnung	Telegrammspeicherung mit Datenkonvertierung für Wireshark.
Modbus/TCP	Zeitmessung mit Hardware Filter	Antwortzeit, Durchlaufzeit, Zykluszeit.
	Telegrammaufzeichnung	Telegrammspeicherung mit Datenkonvertierung für Wireshark.
	Netzlast	Netzwerkanlauf und Ping.

Tabelle 2: Übersicht der Messbeispiele

© Hilscher, 2008-2012

3 Voraussetzungen zur Durchführung der Messungen

3.1 Hardware und Software Installation

1. Die PC-Karte cifX und die zugehörige Software SYCON.net muss installiert sein. Details zur Anwendung entnehmen Sie bitte dem Benutzerhandbuch PC-Karten cifX.
2. Die netANALYZER Hardware und Software muss installiert sein. Details zur Anwendung der netANALYZER Software entnehmen Sie bitte dem *Benutzerhandbuch netANALYZER*.

Weitere Dokumente

Beachten Sie insbesondere auf die zu diesem Kit gehörende Dokumentation *Benutzerhandbuch Real-Time-Ethernet-Kit Installation, Bedienung und Konfiguration*. Im genannten Dokument wird auf die Hardware- und Softwareinstallation der einzelnen Komponenten (CIFX 50-RE und NXIO 50-RE) eingegangen. Die darin beschriebenen Anweisungen sind Vorraussetzungen zur Durchführung dieser Messungen und Datenaufzeichnungen.

Details der Freeware Software wie z. B. Wireshark, die hier zur Anwendung kommt, entnehmen Sie bitte der Dokumentation des entsprechenden Produktes.

3.2 Aufzeichnung der Datentelegramme

Um die aufgezeichneten Dateninhalte anzuzeigen, muss ein Netzwerkmonitoring-Programm installiert sein, welches das WinPcap-Format unterstützt, wie z. B. Wireshark (Wireshark is "free software"). Wireshark kann unter der Internetadresse: http://www.wireshark.org/ bzw. http://www.wireshark.org/download.html bezogen werden. In Wireshark ist ein spezieller Hilscher-Dissector integriert.

Hinweis: GPIO-Events der NANL-C500-RE-Karte werden von Wireshark ab Version 1.0.0 dekodiert. Erscheint in Wireshark die Anzeige nach einer Neuinstallation als „Hilscher- netANALYZER-GPIO-Event“ nicht, dann muss das entsprechende Protokoll zunächst einmalig im Wireshark aktiviert werden.

Hinweis: In Wireshark Versionen vor 1.7.1 ist zusätzlich ein Plugin zu installieren, welches sich auf der netANALYZER-DVD befindet. Siehe hierzu auch Abschnitt 14.3 **Anzeigen und Einstellungen in Wireshark** im *Benutzerhandbuch **netANALYZER** Rev. 12.*

© Hilscher, 2008-2012

Hinweis: Enthält eine .pcap Dateien einen netANALYZER Info Block und ist das Plugin in Wireshark (Version ≤ 1.6) nicht oder nicht korrekt installiert, so könnte Wireshark die vorhandenen Zusatzdaten am Ende des Telegramms fehl interpretieren und ein fehlerhaftes Telegramm anzeigen. Deaktivieren Sie in diesem Fall entweder die Generierung des Info Block oder besser installieren Sie das netANALYZER-Plugin.

Ein vorhandener Info Block bei nicht installiertem Plugin ist an der Kennung „netANALYZER frame info block“ am Ende des Telegramms zu erkennen.

```
0000   01 0e cf 00 01 02 00 b2 23 34 45 00 88 92 00 80   ........#4E.....
0010   e7 90 3f 3b 00 00 00 00 00 06 21 38 04 89 00 00   ..?;......!8....
0020   00 00 00 00 02 16 00 00 00 00 00 00 00 00 00 00   ................
0030   00 00 00 00 00 00 00 00 00 00 00 00 04 0a 00 00   ................
0040   00 00 00 09 38 44 4c 00 06 06 00 00 00 00 00 00   ....8DL.........
0050   08 06 00 00 00 00 00 00 00 00 db 00 00 01 6e 65   ..............ne
0060   74 41 4e 41 4c 59 5a 45 52 20 66 72 61 6d 65 20   tANALYZER frame
0070   69 6e 66 6f 20 62 6c 6f 63 6b 01 00 00 00 00 00   info block......
```

Im folgenden sind einige Messbeispiele für unterschiedliche Real-Time-Ethernet-Protokolle beschrieben. Es ist nur eine kleine Auswahl aus dem Messmöglichkeiten mit dem netANALYZER dargestellt, um das Prinzip der Anwendung aufzuzeigen.

Diese Messbeispiele sind mit den Hardwarekomponenten CIFX 50-RE, NXIO 50-RE und netANALYZER NANL-C500-RE und zugehörigen Kabeln aufgebaut.

3.3 netANALYZER einrichten

➢ Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

➢ Das Hauptfenster erscheint.

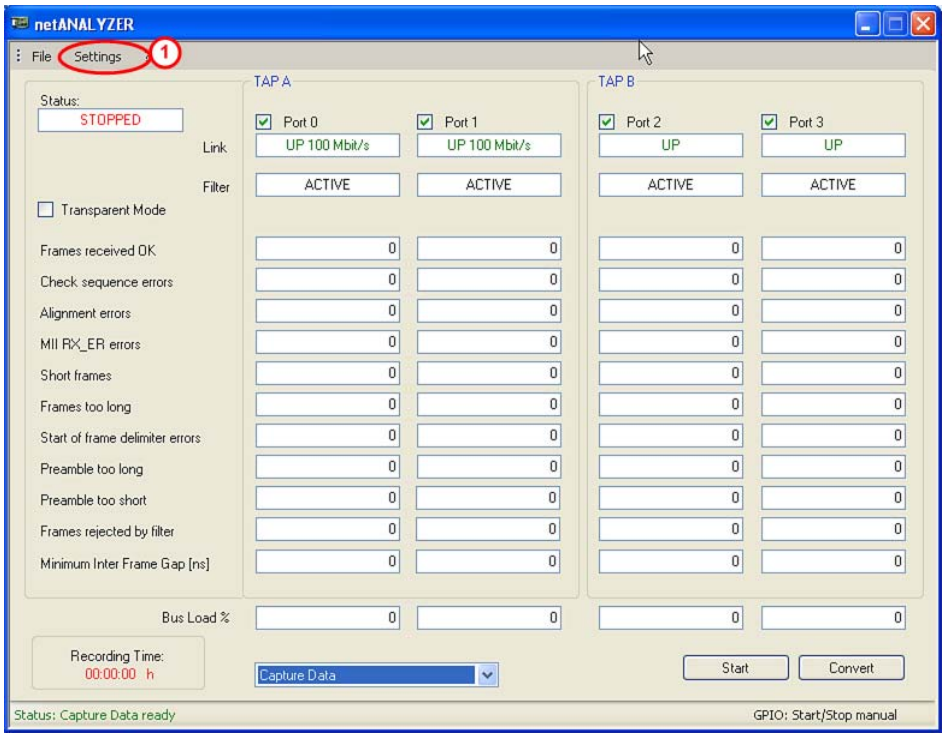


Abbildung 1: netANALYZER Startbild

© Hilscher, 2008-2012

3.3.1 Einstellungen für die Telegrammaufzeichnung

➢ Wählen Sie **Settings > File Settings** ① (siehe Abbildung 1).

➢ Das Fenster zum Konfigurieren der Pfade und den Dateinamen der .hea-Dateien erscheint.

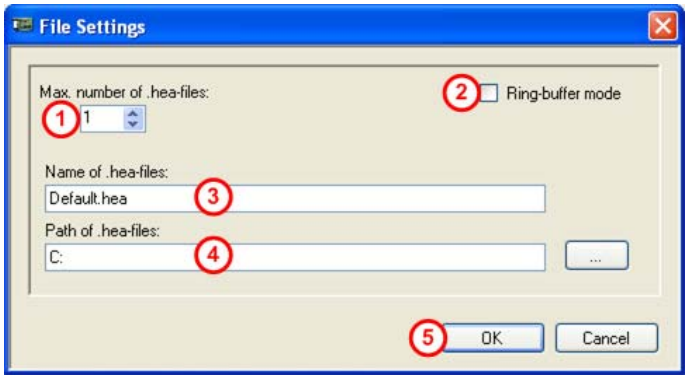


Abbildung 2: netANALYZER File Settings

Bedienelement		Erläuterung	Wertebereich / Wert
①	Max. number of .hea-files	Maximale Anzahl **.hea*-Dateien, die abgelegt werden soll, bevor die Aufzeichnung abgebrochen wird. Die max. Größe einer .hea-Datei ist 1GB.	1 … 100
②	Ring-buffer mode	Wenn angehakt, werden die Aufzeichnungsdaten im Ring-Puffer gespeichert. Wenn nicht angehakt, werden die Aufzeichnungsdaten in einem Stack-Puffer abgelegt (Stack-Puffer-Modus). Hierbei wird die Aufzeichnung dann automatisch beendet, wenn alle (unter ① angegebene Anzahl) .hea-Dateien voll sind.	angehakt / nicht angehakt, Default: angehakt
③	Name of .hea-files	Bezeichnung für **.hea*-Dateien.	1 .. 255 Zeichen
④	Path of .hea-files	Vom Bediener zu definierender Pfad, unter welchem der netANALYZER-Treiber die Binär-Datei (**.hea*) ablegen soll.	
⑤	OK	Die Einstellungen werden gespeichert und das Fenster geschlossen.	

Tabelle 3: Beschreibung File Settings

In diesem Bedienungsfenster legen Sie fest, wie viele Dateien wo für eine Aufzeichnung angelegt werden.

Beachten Sie hierzu auch Abschnitt 8.4 „Dateieinstellungen vornehmen“ im Benutzerhandbuch *netANALYZER Installation, Bedienung und Hardware-Beschreibung.*

© Hilscher, 2008-2012

3.4 Skalierungen im Timing-Analyse Fenster

3.4.1 Skalierung mit den Schiebereglern

Sie haben die Möglichkeit, die grafische Darstellung in den Zeitachsen zu spreizen bzw. zu komprimieren. Die X-Zeitachse im Historienfenster ist am bedeutendsten.

➢ Schalten Sie dazu die **Auto Scale** Funktion (7) aus.

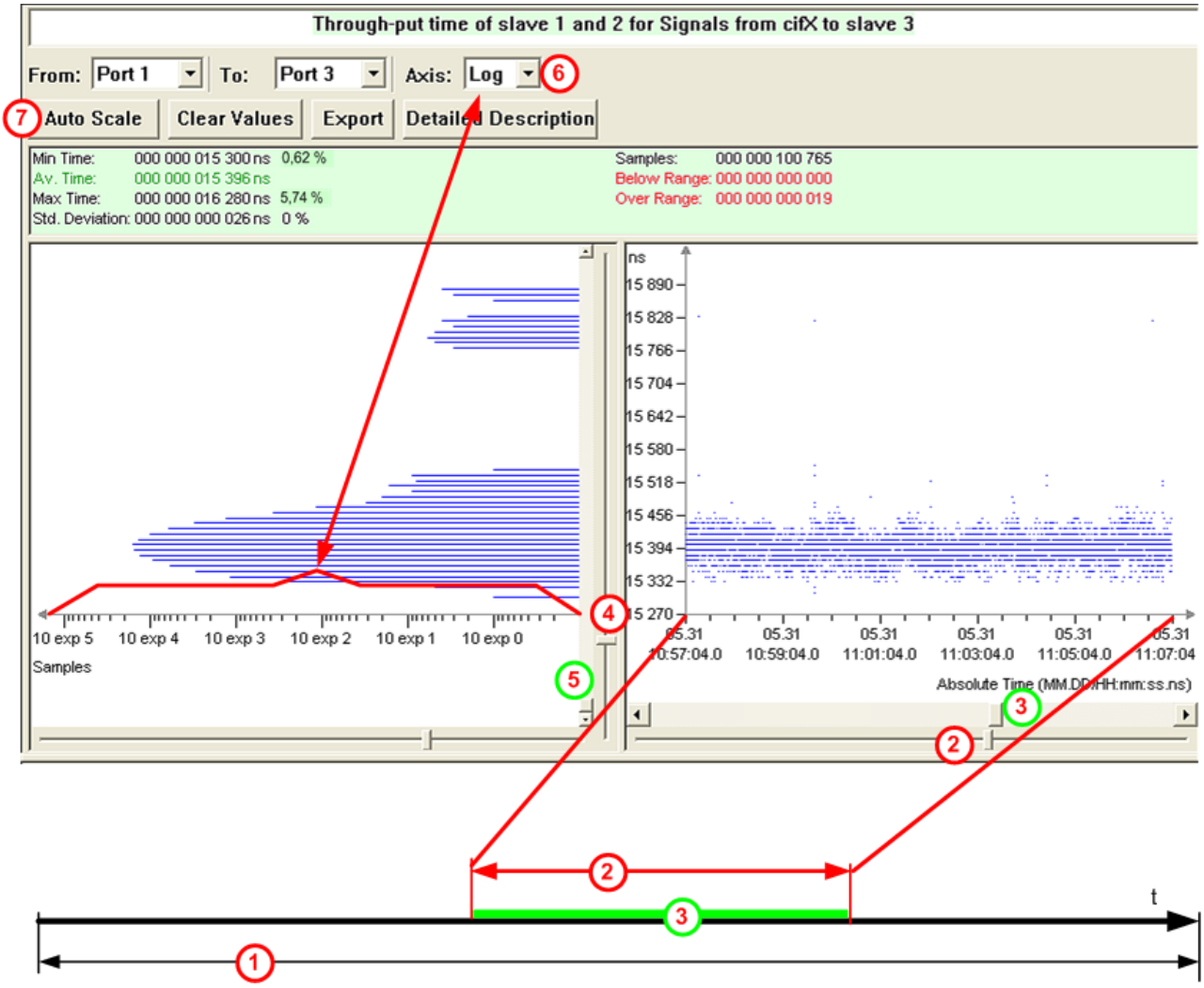


Abbildung 3: Timing-Analyse, Skalierung ändern

Die Zeitachse (1) stellt in der obigen Grafik den gesamten Messzeitraum dar.

Mit dem Schieberegler (2) läst sich die Weite des Darstellungszeitraums verändern.

Mit dem Schieberegler (3) läst sich die Position des Darstellungszeitraums im Messzeitraum verändern.

Entsprechendes gilt auch für die Y-Zeitachse. Hier wird die Darstellungsbreite mit dem Schieberegler (4) eingestellt, und die Darstellungsposition auf dem Zeitstrahl mit dem Schieberegler (5). Hier können die Messereignisse sehr schnell aus dem Darstellungsbereich auswandern. Mit einem Klick auf **Auto Scale** (7) wird der Anzeigebereich wieder über die Ereignisse gelegt.

© Hilscher, 2008-2012

Im Histogramm kann die X-Achse zwischen linearer und logarithmischer Skalierung mittels der Auswahl **Axis** ⑥ umgestellt werden.

Alle 3 Achsen der obigen Abbildung können mittels **Auto Scale** ⑦ so eingestellt werden, dass alle Messereignisse im Anzeigebereich liegen.

3.4.2 Skalierung mit der Maus

Bei gedrückter linker Maustaste können Sie die Bereichsauswahl zoomen.

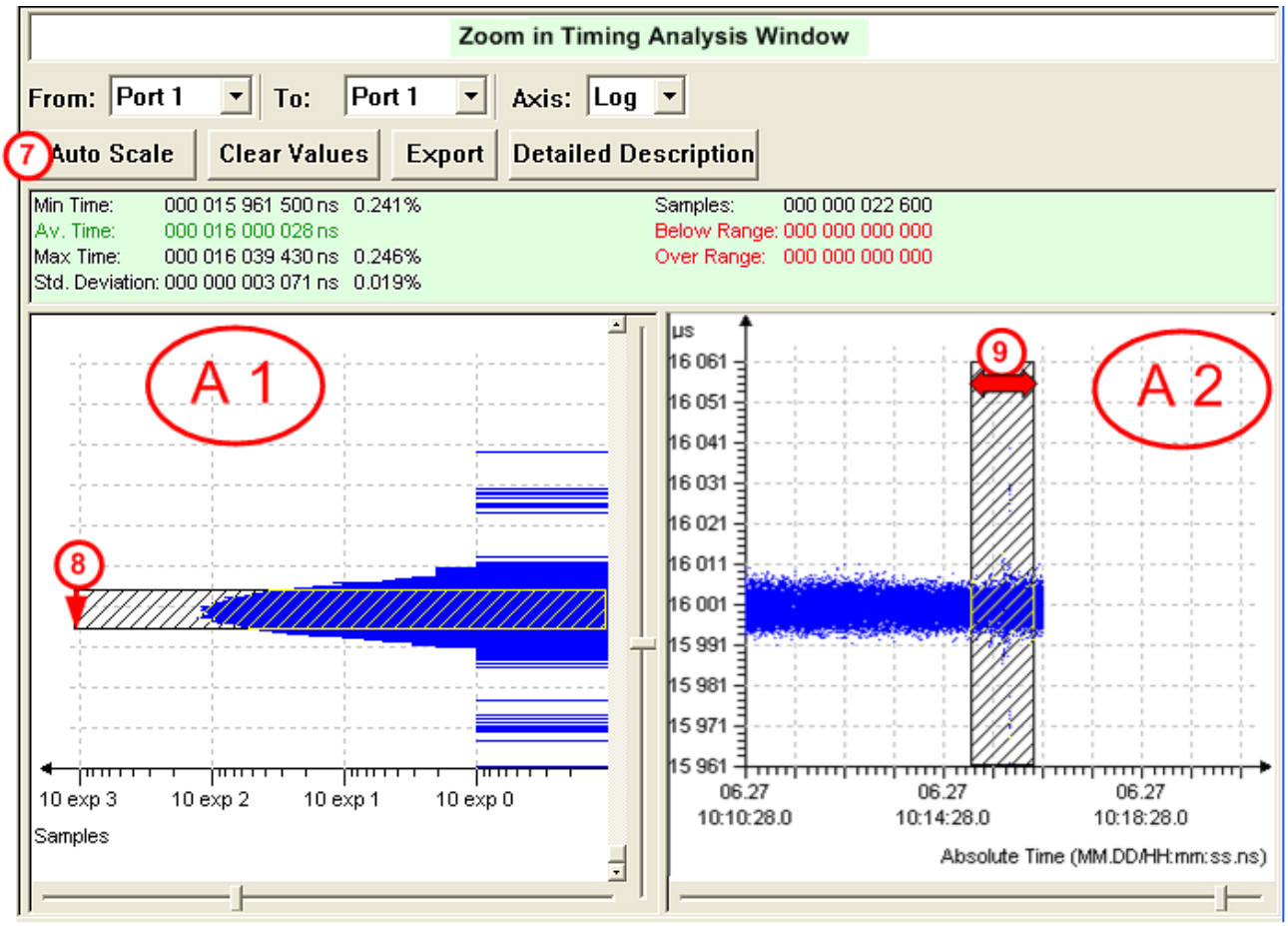


Abbildung 4: Timing Analyse, zoomen mit der Maus

- ➢ Schalten Sie **Auto Scale** ⑦ aus.
- ➢ Markieren Sie mit gedrückter linker Maustaste im Fensterbereich **A 1** horizontal ⑧ oder im Fensterbereich **A 2** vertikal einen Bereich ⑨. Der Bereich wird schraffiert dargestellt.
- ➢ Nach dem Loslassen der Maustaste wird der Bereich in beiden Teilfenstern gezoomt.
- ➢ Um in die Ursprungsdarstellung zurück zu kommen, schalten Sie **Auto Scale** ⑦ wieder ein.

© Hilscher, 2008-2012

4 PROFINET IO Analyse

Beispielhaft werden hier folgende Messungen durchgeführt:

- Messung der Zykluszeit, mit der der Controller ein Telegramm zu einem Device sendet,
- Messung der Telegrammdurchlaufzeit durch Device 1 für das Telegramm des Controllers zum Device 2,
- Messung der Netzlast von PROFINET-Telegrammen.

4.1 Hardware-Aufbau

Für diese Beispielmessung wird folgender Hardware-Aufbau benötigt.

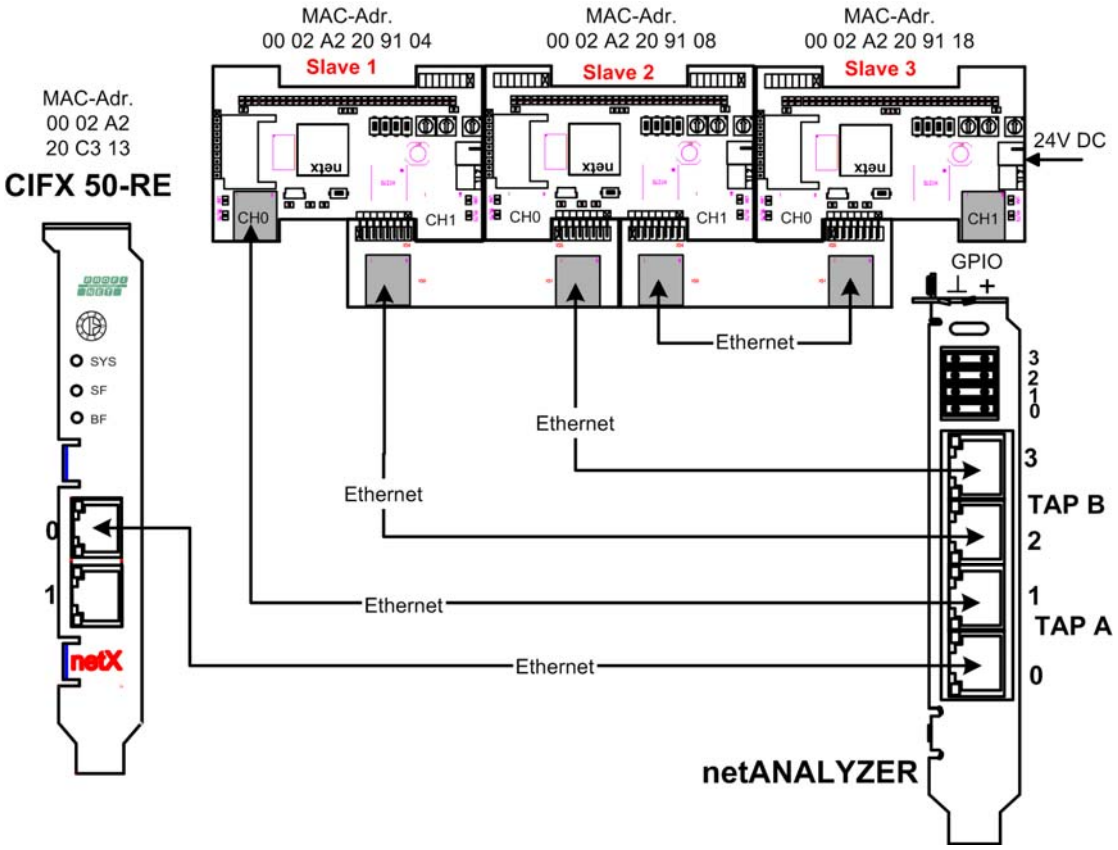


Abbildung 5: PROFINET IO Analyse, Hardware-Aufbau

Die für den in diesem Aufbau geltenden MAC-Adressen sind oberhalb der Komponenten angegeben.

Beachten Sie bitte, dass die jeweilige MAC-Adresse auf der Welt einmalig ist. Daher haben die Geräte in Ihrem Messaufbau andere MAC-Adressen. Brücksichtigen Sie dieses bitte bei Ihren Filtereinstellungen.

Hinweis: Die Einstellungen für die PC-Karte cifX und die NXIO 50 Boards müssen entsprechend Abschnitt 6.2 des *Benutzerhandbuch Real-Time-Ethernet-Kit Installation, Bedienung und Konfiguration* vorgenommen worden sein.

© Hilscher, 2008-2012

4.2 Zeitmessungen vorbereiten und durchführen

Hinweis: Die PC-Karte cifX und die NXIO-Boards verfügen über eine Autocrossover-Funktionalität. Daher ist ein Vertauschen der Kabel am netANALYZER am TAP A (Port 0 und Port 1) sowie am TAP B (Port 2 und Port 3) ohne Bedeutung. Somit sind auch bei der Anzeige der Analysewerte die Portbezeichnungen 0/1 bzw. 2/3 als vertauschbar zu betrachten.

Hinweis: Hier sind nur die für diesen Messaufbau unmittelbar erforderlichen Einstellungen des netANALYZERs beschrieben. Detaillierte Informationen über die Einstell- und Aufzeichnungsmöglichkeiten der Software entnehmen Sie bitte der Dokumentation *Benutzerhandbuch netANALYZER*.

4.2.1 Zeitmessung vorbereiten

Die Zykluszeit der Telegramme der PC-Karte cifX zum Device 2 und die Gerätedurchlaufzeit von Device 1 soll für diese Telegramme gemessen werden.

- Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.
- Nach der Auswahl der netANALYZER-Karte gelangen Sie ins Hauptfenster des netANALYZERs.

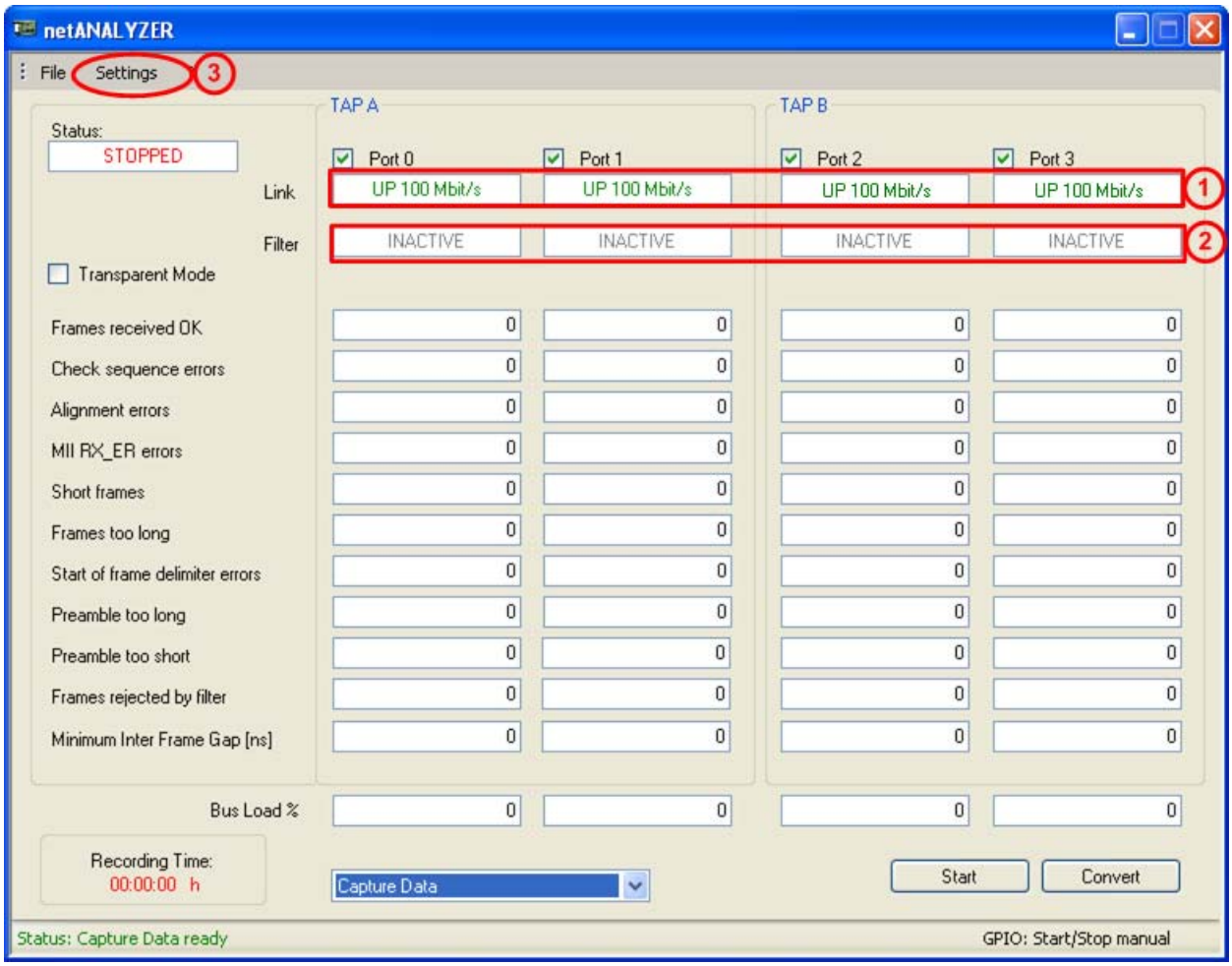


Abbildung 6: netANALYZER Hauptfenster

© Hilscher, 2008-2012

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 16 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus als **UP mit Datenrate** (1) dargestellt oder bei älteren netANALYZER-Karten bei TAP B nur mit **UP** gekennzeichnet.

Ob auf diesem Eingang ein Filter aktiv ist, können Sie in der Zeile **Filter** (2) sehen (INACTIVE = kein Filter).

4.2.2 Filter einstellen

➢ Wählen Sie **Settings > Filter Settings** (3).

➢ Das Filter-Fenster erscheint.

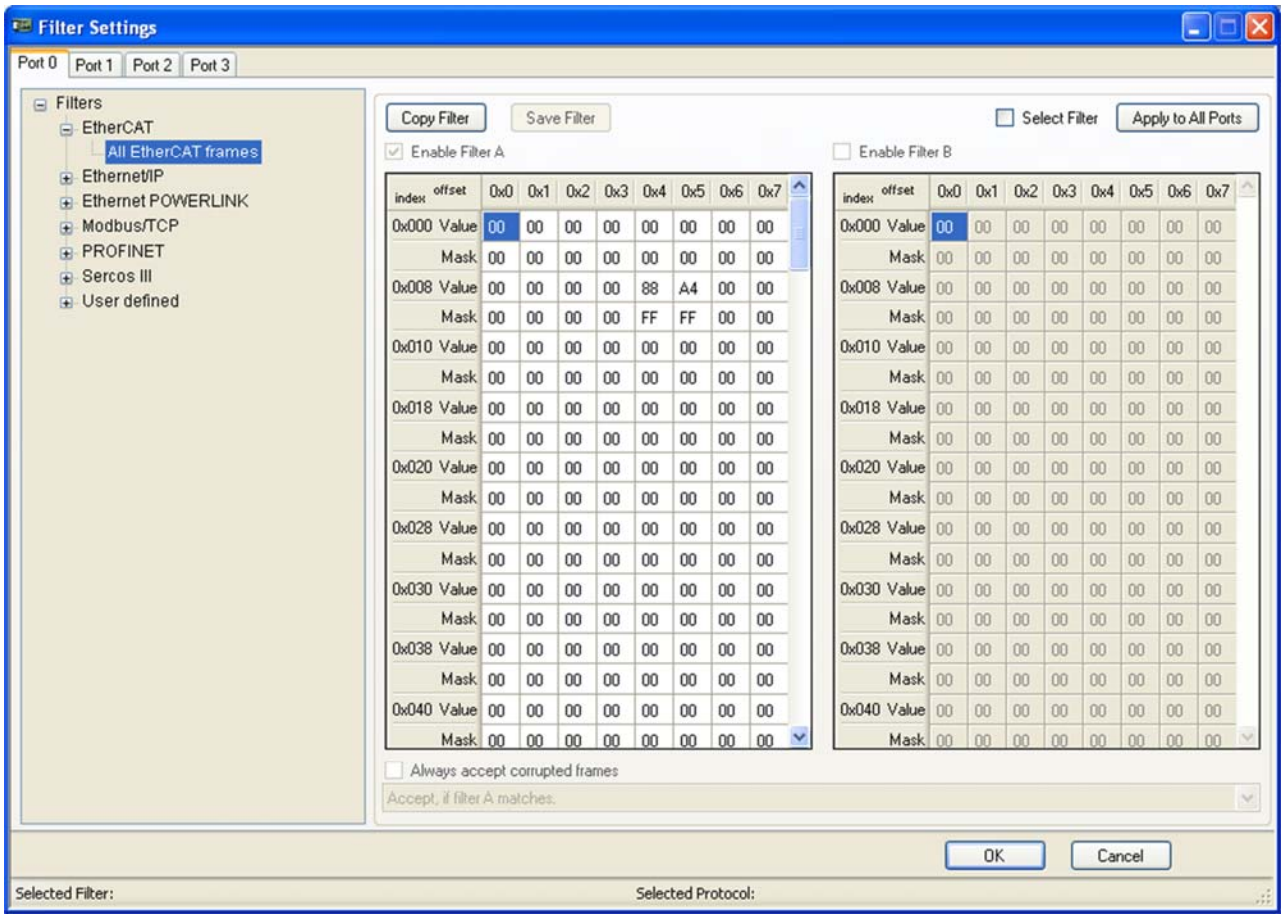

Filter Settings
Port 0
Port 1
Port 2
Port 3
Filters
EtherCAT
All EtherCAT frames
Ethernet/IP
Ethernet POWERLINK
Modbus/TCP
PROFINET
Sercos III
User defined
Copy Filter
Save Filter
Select Filter
Apply to All Ports
Enable Filter A
Enable Filter B
index offset 0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7
0x000 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x008 Value 00 00 00 00 88 A4 00 00
Mask 00 00 00 00 FF FF 00 00
0x010 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x018 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x020 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x028 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x030 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x038 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x040 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
Always accept corrupted frames
Accept, if filter A matches.
OK
Cancel
Selected Filter:
Selected Protocol:

Abbildung 7: netANALYZER Filtereinstellungen (1)

© Hilscher, 2008-2012

Gehen Sie wie folgt vor, um die für die Messung erforderlichen Einstellungen zu machen.

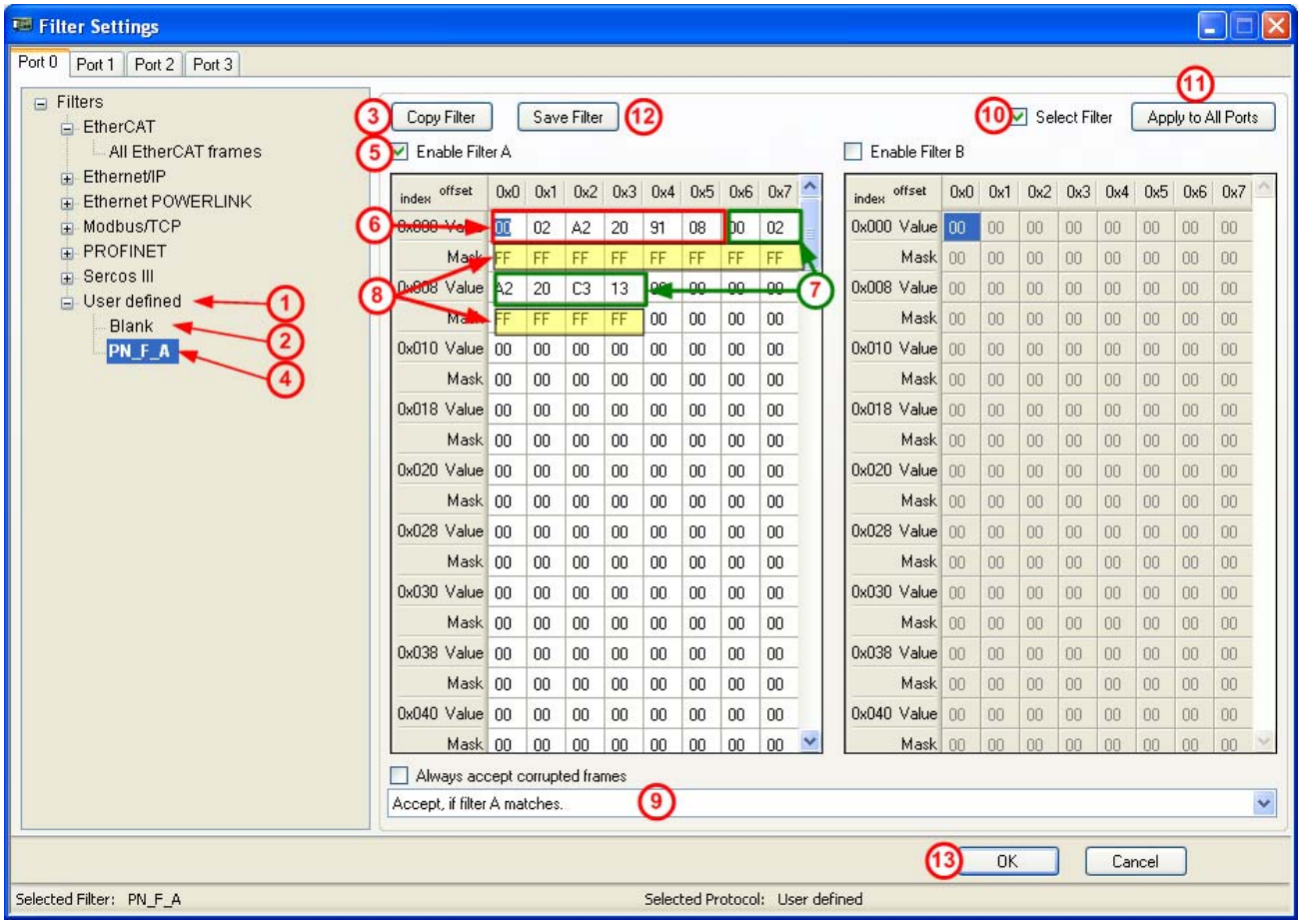


Abbildung 8: netANALYZER Filtereinstellungen (2)

- Machen Sie einen Doppelklick auf den Menüeintrag **Filters > User defined** (1).

- Es erscheint der Eintrag **Blank** (2).

- Wählen Sie die Zeile **Blank** (2) mit der rechten Maustaste aus.

- Klicken Sie **Copy Filter** (3).

- Es erscheint der neue Eintrag (4) unter der Filterauswahl.

- Vergeben Sie einen neuen Namen (hier PN_F_A) für den anzulegenden Filter.

- Haken Sie **Enable Filter A** (5) an.

Ziel-MAC-Adresse

- Tragen Sie in den ersten 6 Byte der Value-Zeile des Filters (6) die Ziel-MAC-Adresse des Gerätes ein, an das die Daten gesendet werden (hier 00 02 A2 20 91 08, Device 2).
  Achten Sie darauf, dass Sie die MAC-Adressen Ihrer verwendeten Geräte eintragen.

© Hilscher, 2008-2012

Quell-MAC-Adresse

- Tragen Sie von Byte 0x6 bis 0xB der Value-Zeile ⑦ die Quelladresse der Datenpakete ein (hier 00 02 A2 20 C3 13, cifX). Achten Sie darauf, dass Sie die MAC-Adressen Ihrer verwendeten Geräte eintragen.

Filtermaske

- Tragen Sie in die **Mask** Felder ⑧ unter der Ziel- und Quelladresse „FF“ ein, damit jedes Bit in der Ziel- und Quelladresse beim Vergleich berücksichtigt wird.
- Achten Sie darauf, dass in der angegebenen Auswahlzeile der Eintrag **Accept, if Filter A matches** ⑨ eingestellt ist, damit nur die Datenpakete berücksichtigt werden, auf die die Auswahl zutrifft.
- Klicken Sie **Select Filter** ⑩.

  Klicken Sie **Apply to All Ports** ⑪, damit diese Filtereinstellungen an allen Ports wirksam wird.
- Speichern Sie die Filtereinstellungen mit **Save Filter** ⑫.
- Verlassen Sie die Filtereinstellungen mit **OK** ⑬.

Hinweis: Passen Sie für Ihren Messaufbau die MAC-Adressen entsprechend der von Ihnen verwendeten Geräte an.

© Hilscher, 2008-2012

Sie gelangen ins Hauptfenster.

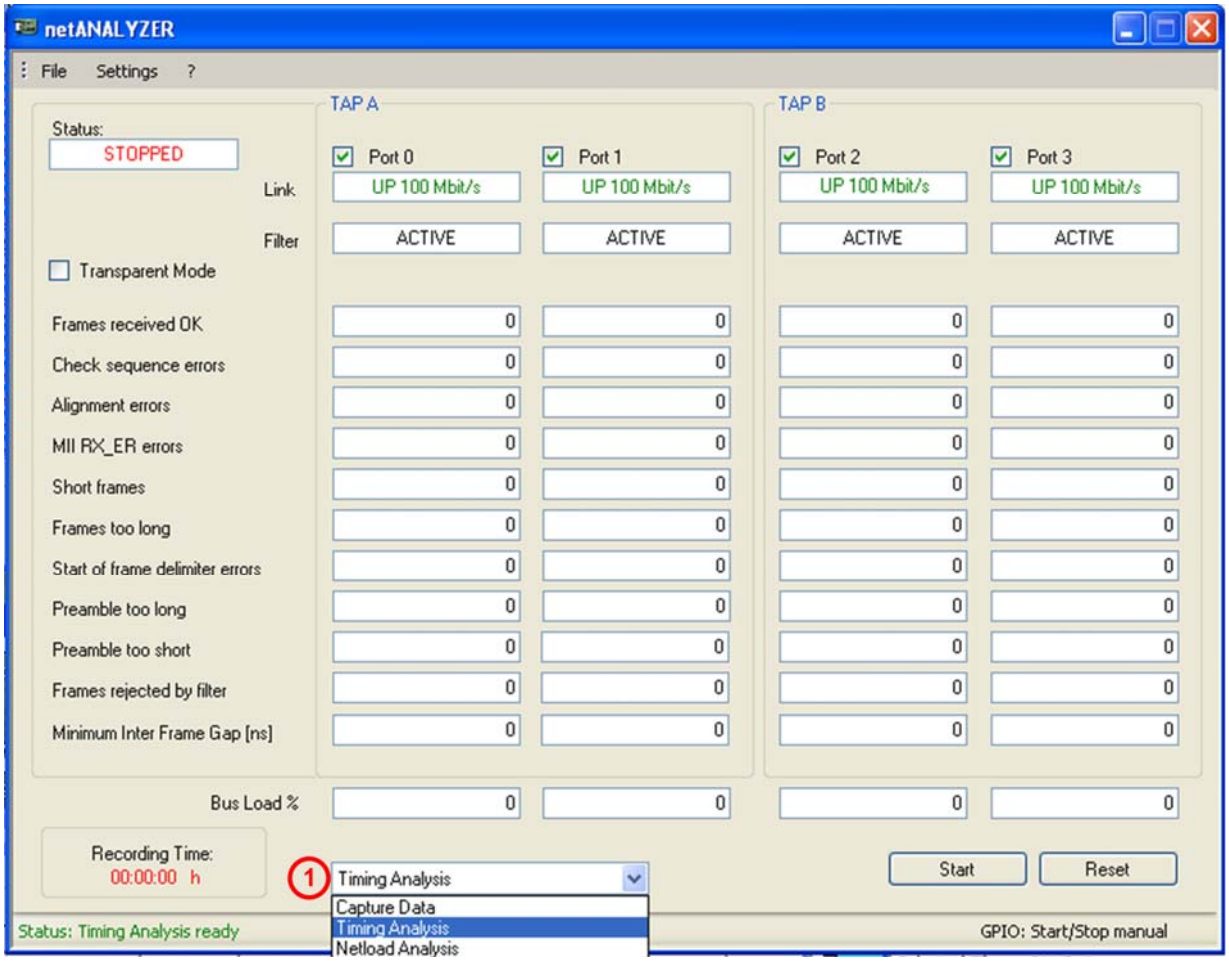


Abbildung 9: netANALYZER, Auswahl Timing-Analyse

➢ Wählen Sie **Timing Analysis** (1).

© Hilscher, 2008-2012

Es öffnet sich im Vordergrund das Fenster zur grafischen Darstellung der Zeitanalyse (Timing Analysis).

Abbildung 10: netANALYZER Messfenster

Das Timing-Analysis-Fenster unterteilt sich in 4 Unterfenster, die wiederum 2 Teilfenster (Histogramm und Historie) beinhalten. Im weiteren Verlauf dieses Messaufbaus wird in der Regel immer nur ein Unterfenster angesprochen.

Die Größe der Einzelfenster können Sie durch ziehen des Kreuzungspunktes der Fensterteilungslinien verändern.

Sie können sich auch nur das Historie- oder Histogramm-Fenster anzeigen lassen. Dieses können Sie im Hauptfenster des netANALYZERs unter **Settings > Analysis Configuration** einstellen.

4.2.3 Signalflussrichtung ermitteln

- Klicken Sie in das Hauptfenster vom netANALYZER.
- Klicken Sie **Start** und anschließend auf **Stop** (diese befindet sich jetzt an der Position der Schaltfläche **Start**), damit einige Telegramme aufgezeichnet werden.

Dieses ist erforderlich, um festzustellen auf welchen Ports der Analyzerkarte die Telegramme detektiert werden.

© Hilscher, 2008-2012

➢ Das Hauptfenster sollte jetzt wie folgt aussehen.

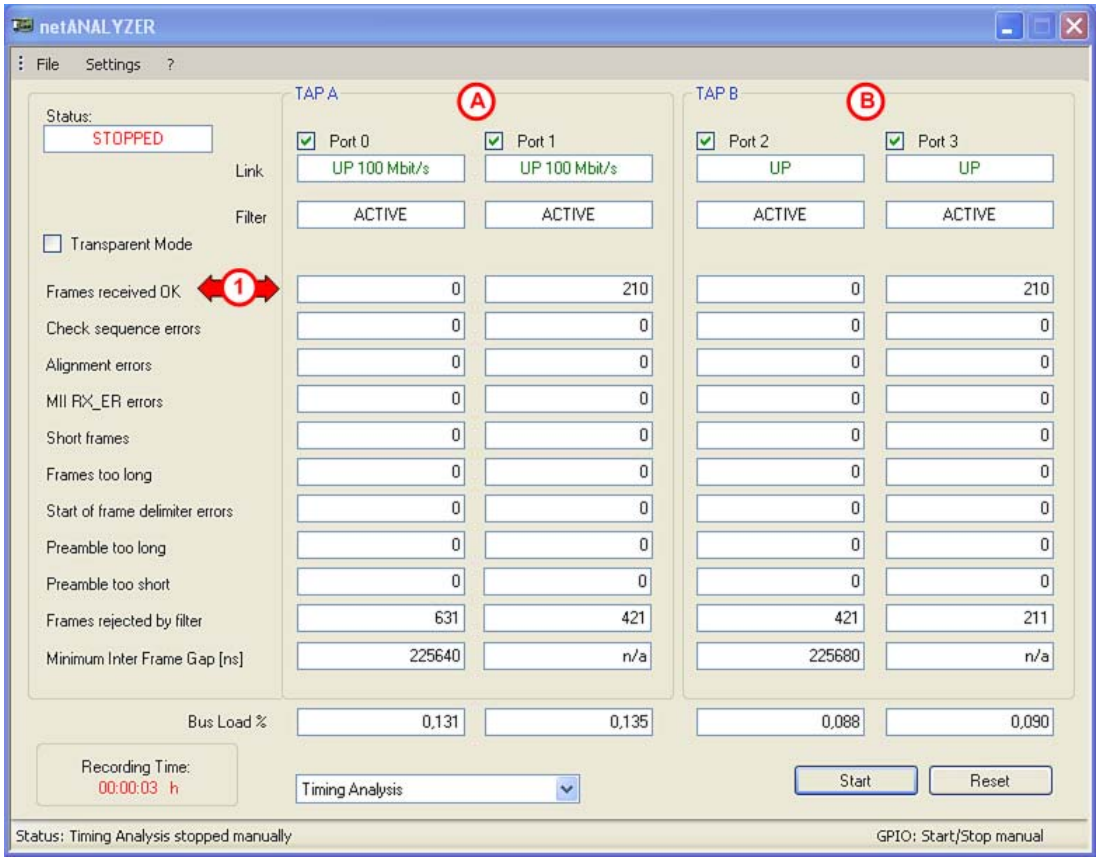


Abbildung 11: netANALYZER, Hauptfenster nach Messzyklus

Unter **TAP A** Ⓐ sind jetzt in der Zeile **Frames received OK** ① unter Port 0 oder Port 1 eine Anzahl größer als 0 zu sehen (hier Port 1). Dieser Port ist für die Einstellungen im Fenster Timing Analysis wichtig, und wird im weiteren Ablauf als „aktiver Port TAP A“ bezeichnet.

Unter **TAP B** Ⓑ sind jetzt in der Zeile **Frames received OK** ① unter Port 2 oder Port 3 eine Anzahl größer als 0 zu sehen (hier Port 3). Dieser Port ist für die Einstellungen im Fenster Timing-Analysis wichtig, und wird im weiteren Ablauf als „aktiver Port TAP B“ bezeichnet.

Hinweis: Durch die Autocrossover-Funktionalität der Ethernet-PHYs der Geräte können bei einem erneutem Start der Kommunikation die Ports 0 und 1 bzw. 2 und 3 gegeneinander vertauscht sein.

➢ Wechseln Sie in das Fenster **Timing Analysis**.

© Hilscher, 2008-2012

4.2.4 Einstellungen in den Analysefenstern

4.2.4.1 Einstellungen für Analysefenster A

Zur Messung der Zykluszeit der Abfrage-Telegramme an Device 2:

➢ Nehmen Sie im Teilfenster A folgende Einstellungen vor.

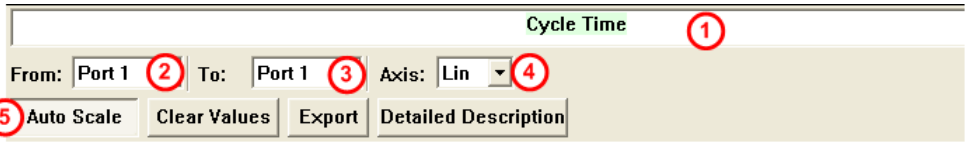


Abbildung 12: netANALYZER Messfenstereinstellungen 1

In dieser Zeile können Sie eine beliebige Bezeichnung für diese Messung eingeben (1).

Hinter **From:** wählen Sie den „aktiven Port TAP A“ (hier **Port 1**) (2) aus, (ermittelt in Abschnitt *Signalflussrichtung ermitteln* auf Seite 22).

Hinter **To:** wählen Sie den „aktiven Port TAP A“ (hier **Port 1**) (3) aus, (ermittelt in Abschnitt *Signalflussrichtung ermitteln* Seite 22).

Mit dieser Einstellung wird die Zykluszeit der (mittels der Filter selektierten) Telegramme gemessen. Auf diesem Port haben wir in der Abbildung 11: die Telegramme an Device 2 detektiert.

Hier kann die Skalierung der Y-Achse zwischen linear und logarithmisch umgeschaltet werden (4).

Achten Sie darauf, dass für die Zeitachse **Auto Scale** (5) eingestellt ist. Damit stellen Sie sicher, dass die Ergebnisse immer im sichtbaren Bereich des Fensters angezeigt werden.

4.2.4.2 Einstellungen für Analysefenster B

Hier soll die Telegrammdurchlaufzeit durch Device 1 gemessen werden.

➢ Nehmen Sie dazu folgende Einstellungen vor:

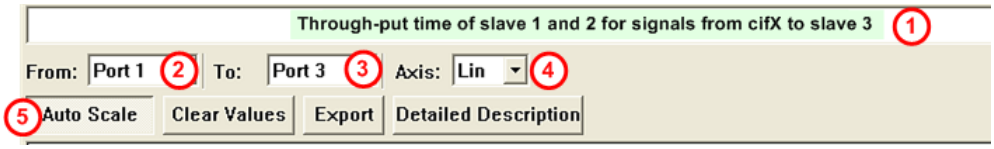


Abbildung 13: netANALYZER Messfenstereinstellungen 2

In dieser Zeile können Sie eine beliebige Bezeichnung für diese Messung eingeben (1).

Hinter **From:** wählen Sie den „aktiven Port TAP A“ (hier **Port 1**) (2) aus, (ermittelt in Abschnitt *Signalflussrichtung ermitteln* Seite 22).

Hinter **To:** wählen Sie den „aktiven Port TAP B“ (hier **Port 3**) (3) aus, (ermittelt in Abschnitt *Signalflussrichtung ermitteln* Seite 22).

Achten Sie darauf, dass für die Zeitachse **Auto Scale** (5) eingestellt ist. Damit stellen Sie sicher, dass die Ergebnisse immer im sichtbaren Bereich des Fensters angezeigt werden.

© Hilscher, 2008-2012

4.2.5 Messung durchführen

➢ Klicken Sie im Hauptfenster des netANALYZERS.

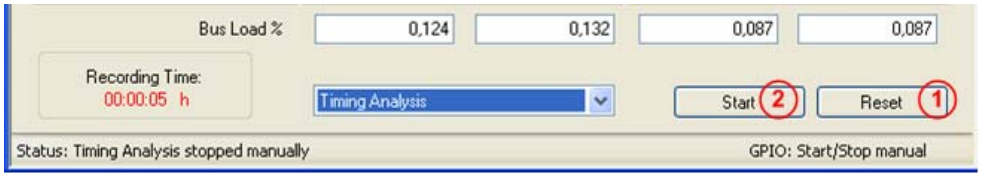


Abbildung 14: netANALYZER Hauptfenster, Start, Reset

➢ Klicken Sie auf **Reset** (1). Damit werden die bisher aufgezeichneten Zeitdaten gelöscht.

➢ Klicken Sie auf **Start** (2), um die Analyse zu starten.

↬ Die Schaltfläche **Start** wird zur Schaltfläche **Stop**.
Verfolgen Sie unmittelbar die grafische Darstellung der Messwerte. Noch während der laufenden Aufzeichnung können Sie mit der Auswertung beginnen.

Im hier dargestelltem Beispiel wurde eine Auswertung über ca. 30 Minuten gemacht. Dabei entstanden die folgenden Grafiken:

➢ Warten Sie die Zeit, in der Sie Telegramme auswerten möchten.

➢ Klicken Sie **Stop**.

↬ Im Fenster A des Timing Analysis-Fensters (Auswertung der Zykluszeit) finden Sie jetzt folgende Informationen:

4.2.5.1 Messergebnis im Teilfenster A

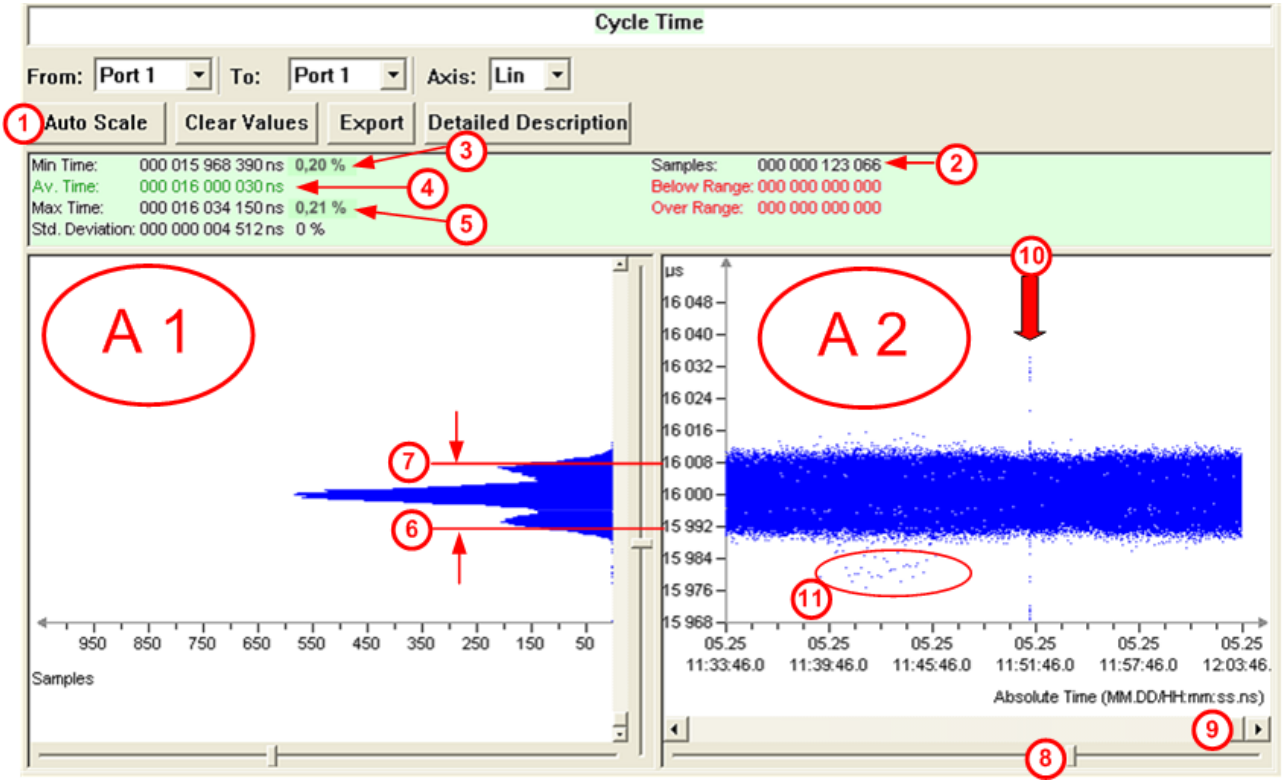


Abbildung 15: netANALYZER PROFINET IO Zykluszeitmessung, Auto-Scale

➢ Schalten Sie „**Auto Scale**“ (1) aus, um sich mit den Schiebereglern in den Teilbildern die optimale Auflösung und Zeitbereich einstellen zu können.

© Hilscher, 2008-2012

② Die Anzahl der analysierten Telegramme (123066).

③ Die minimale Zykluszeit in **ns** mit Tausender-Abtrennung, dahinter die Abweichung zur mittleren Zeit in %.

④ Die mittlere Zykluszeit in **ns** mit Tausender-Abtrennung.

⑤ Die maximale Zykluszeit in **ns** mit Tausender-Abtrennung, dahinter die Abweichung zur mittleren Zeit in %.

Die max. und min. Zeiten 16,03 ms ③ und 15,97 ms ④ geben Extremzeiten an. In der Grafik „**A 1**“ (dem Histogramm) ist zu erkennen, dass die meisten Telegramme jedoch in einem wesentlich schmaleren Zeitfenster ca. 15,992 ms ⑥ und 16,008 ms ⑦ liegen.
Im Historien Fenster „**A 2**“ kann man durch verschieben der Schieberegler ⑧ (Auflösung) und ⑨ (Zeitposition) die Zeitlichen Abschnitte finden, in denen die seltenen Ausreißer liegen. Hier mit ⑩ und ⑪ gekennzeichnet.

4.2.5.2 Messergebnis im Teilfenster B

➢ Im Fenster B des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

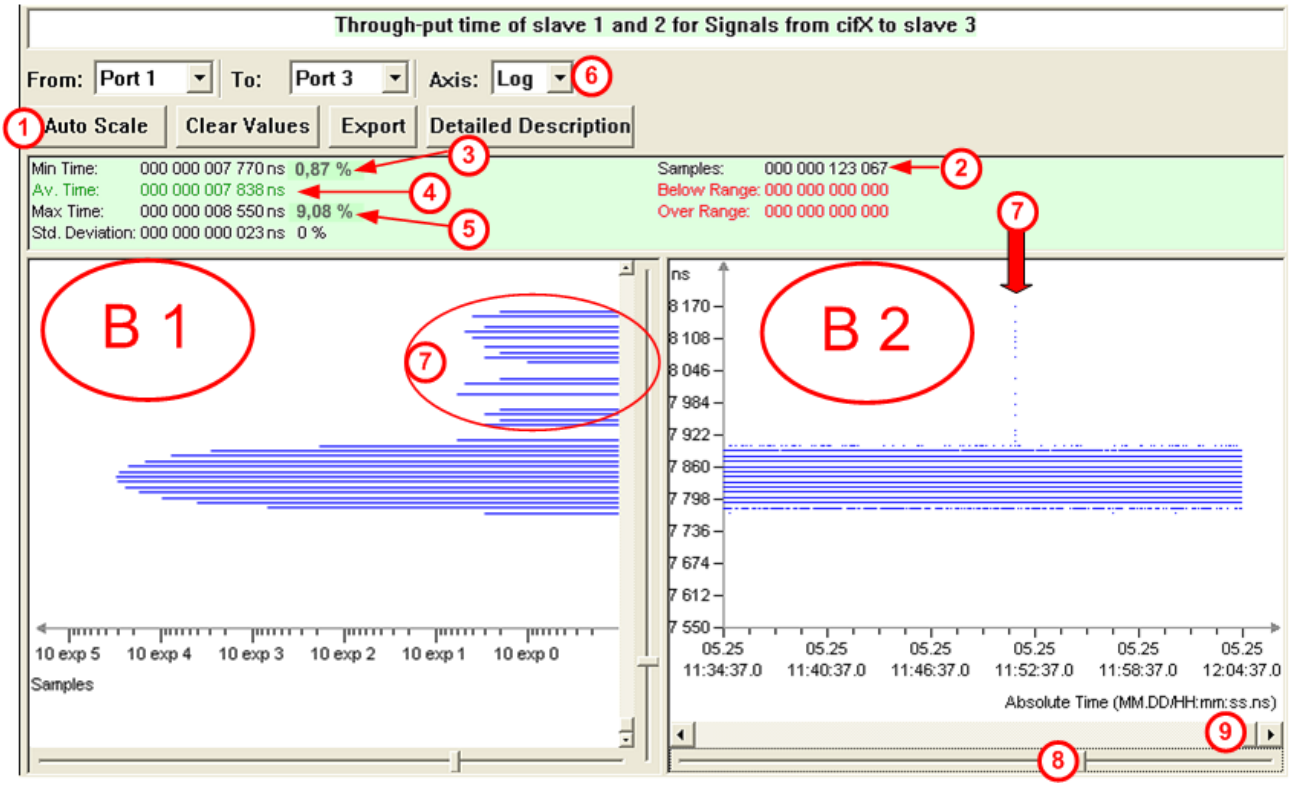


Abbildung 16: PROFINET IO, Device 1 Durchlaufzeit

➢ Schalten Sie **Auto Scale** ① aus, um sich mit den Schiebereglern in den Teilbildern die optimale Auflösung und Zeitbereich einstellen zu können.

② Die Anzahl der analysierten Telegramme (123067).

③ Die minimale Durchlaufzeit in **ns** mit Tausender-Abtrennung und anschließender Prozentangabe zu mittleren Messzeit (hier 7,77 µs und 0,87 %).

© Hilscher, 2008-2012

④ Die mittlere Durchlaufzeit **ns** mit Tausender-Abtrennung (hier 7,838 µs).

⑤ Die maximale Durchlaufzeit **ns** mit Tausender-Abtrennung und anschließender Prozentangabe zu mittleren Messzeit (hier 8,55 µs und 9,08 %).

Diese prozentuale Abweichung erscheint sehr hoch. Stellt man jedoch die **Axis** ⑥ auf logarithmisch, dann kann man in der Grafik „**B 1**“ erkennen, dass es nur sehr wenige Telegramme sind, die diese Abweichung verursachen. In der History-Grafik „**B 2**“ kann man durch verschieben der Schieberegler ⑧ (Auflösung) und ⑨ (Zeitposition) erkennen, dass diese „Ausreißer“ alle in einem kurzen Zeitabstand ⑦ auftreten.

Durch noch weiteres Spreizen der Zeitachse in der History-Grafik kann man auch sehr genau die absolute Zeit der Ereignisse ermitteln.

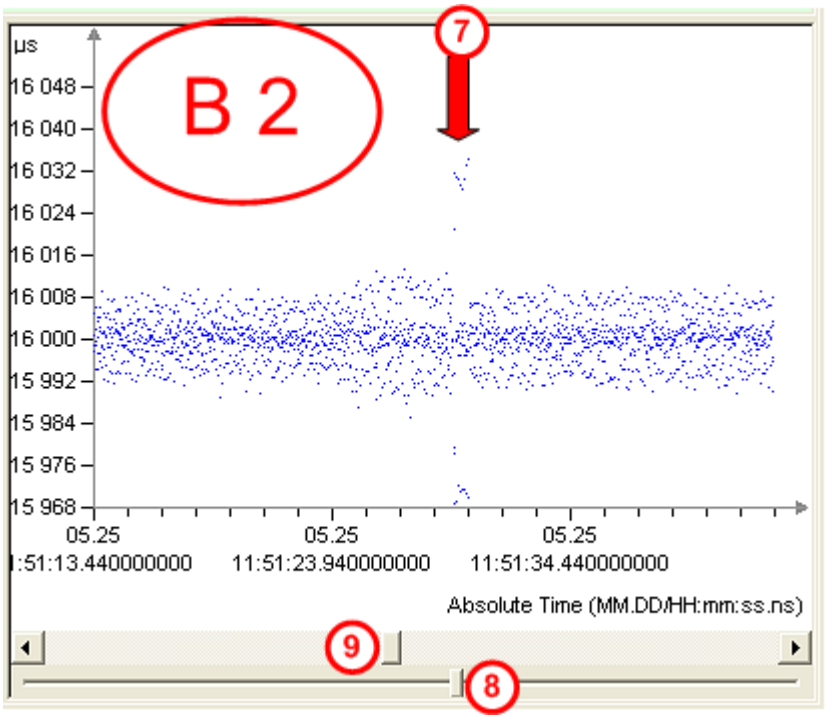


Abbildung 17: PROFINET IO, Device 1 Durchlaufzeit, History extrem gespreizt

© Hilscher, 2008-2012

4.3 Datenaufzeichnungen durchführen

Es sollen die Telegramme der PC-Karte cifX zum Device 2 und die Antworttelegramme vom Device 2 an die PC-Karte cifX aufgezeichnet werden.

Voraussetzungen:

- Der Hardware-Aufbau, wie in *Hardware-Aufbau* auf Seite 16 beschrieben, muss erstellt sein,
- die Einstellungen für die PC-Karte cifX müssen erfolgt sein,
- es muss ein Datenaustausch zwischen der PC-Karte cifX und den Devices erfolgen.

➢ Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

↬ Sie gelangen ins Hauptfenster des netANALYZERs.

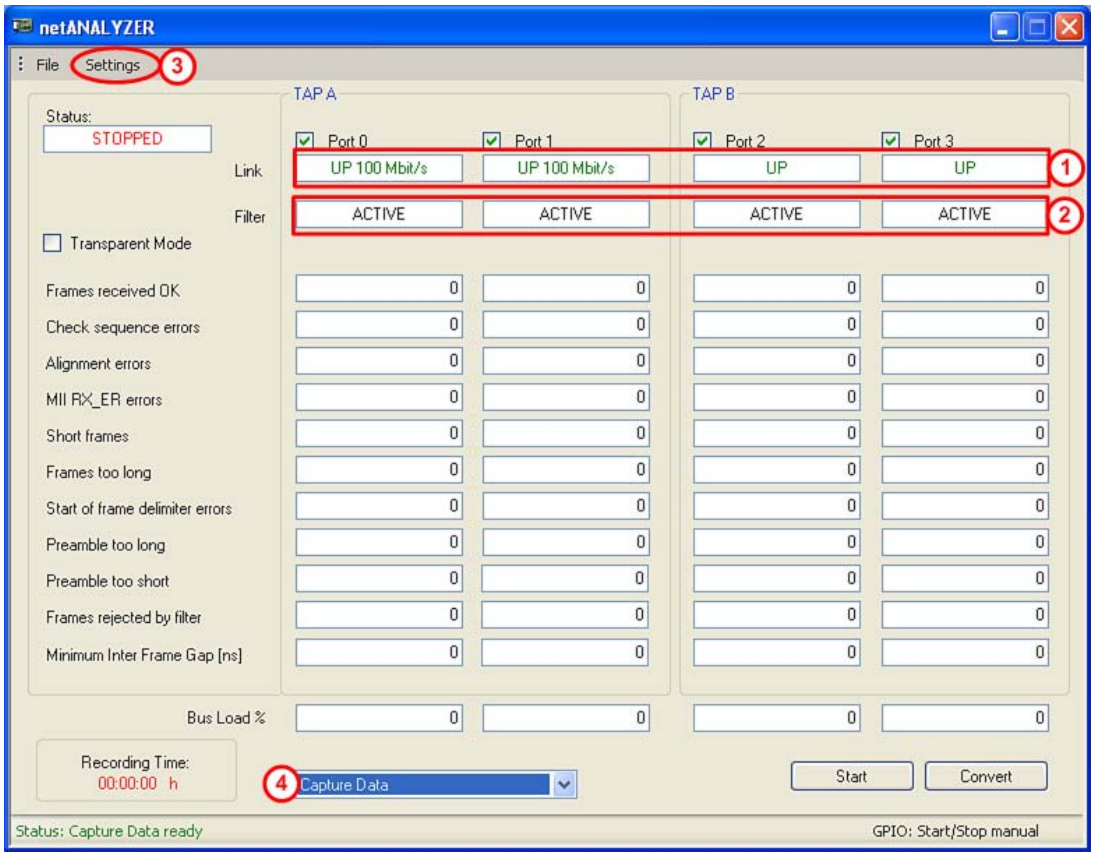


Abbildung 18: Hauptfenster für Telegrammaufzeichnung

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 16 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP** gekennzeichnet.

Sind die Filtereinstellungen aus der Timinganalyse noch aktiv, wird dieses unter ② mit **ACTIVE** gekennzeichnet. Kontrollieren Sie die Filtereinstellungen.

© Hilscher, 2008-2012

➢ Wählen Sie im Hauptfenster **Settings > Filter Settings**.

➢ Das Filter-Fenster erscheint wie folgt.

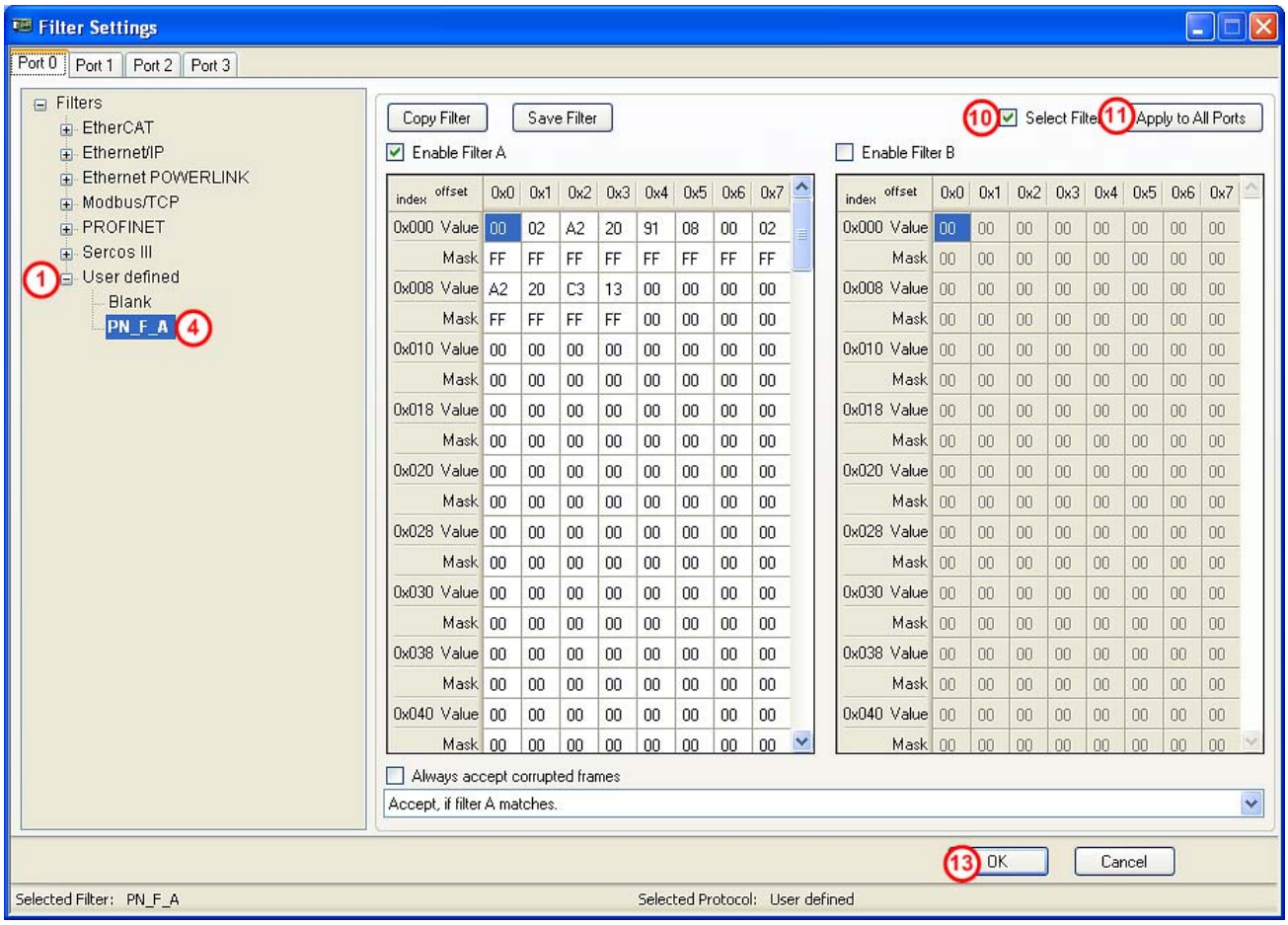

Filter Settings
Port 0
Port 1
Port 2
Port 3
Filters
EtherCAT
EtherNet/IP
Ethernet POWERLINK
Modbus/TCP
PROFINET
Sercos III
User defined
Blank
PN_F_A
1
4
Copy Filter
Save Filter
10
Select Filter
11
Apply to All Ports
Enable Filter A
Enable Filter B
index offset
0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7
0x000 Value 00 02 A2 20 91 08 00 02
Mask FF FF FF FF FF FF FF FF
0x008 Value A2 20 C3 13 00 00 00 00
Mask FF FF FF FF 00 00 00 00
0x010 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x018 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x020 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x028 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x030 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x038 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
0x040 Value 00 00 00 00 00 00 00 00
Mask 00 00 00 00 00 00 00 00
Always accept corrupted frames
Accept, if filter A matches.
13
OK
Cancel
Selected Filter: PN_F_A
Selected Protocol: User defined

Abbildung 19: netANALYZER PROFINET IO Filtereinstellungen

➢ Nehmen Sie die oben dargestellten Einstellungen vor:

➢ Öffnen Sie die **User defined** (1) Filtereinstellung, die Sie in der Timing-analyse angelegt haben.

➢ Wählen Sie den gespeicherten Filter **PN_F_A** (4) wie im Abschnitt *Zeitmessung vorbereiten* auf Seite 17 definiert.

➢ Setzen Sie den Haken bei **Select Filter** (10).

➢ Klicken Sie **Apply to All Ports** (11).

➢ Kontrollieren Sie, dass diese Filtereinstellung für jeden Port gilt.

➢ Verlassen Sie das Fenster mit **OK** (13).

© Hilscher, 2008-2012

Sie kommen zurück ins Hauptfenster.

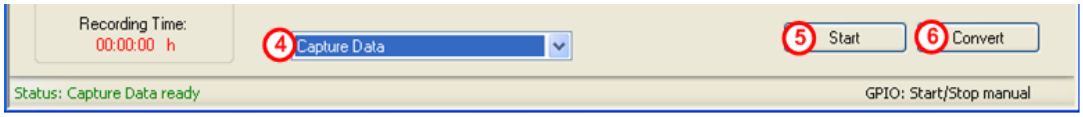


Abbildung 20: Datenaufzeichnung starten

- Stellen Sie sicher, dass **Capture Data** (4) eingestellt ist.
- Klicken Sie **Start** (5), um die Aufzeichnung zu starten.

Die Schaltfläche **Start** (5) wird zur Schaltfläche **Stop** (5).

- Warten Sie bis eine ausreichende Anzahl von Telegrammen aufgezeichnet wurden.
- Klicken Sie **Stop** (5).
- Klicken Sie **Convert** (6).

Es erscheint folgendes Fenster:

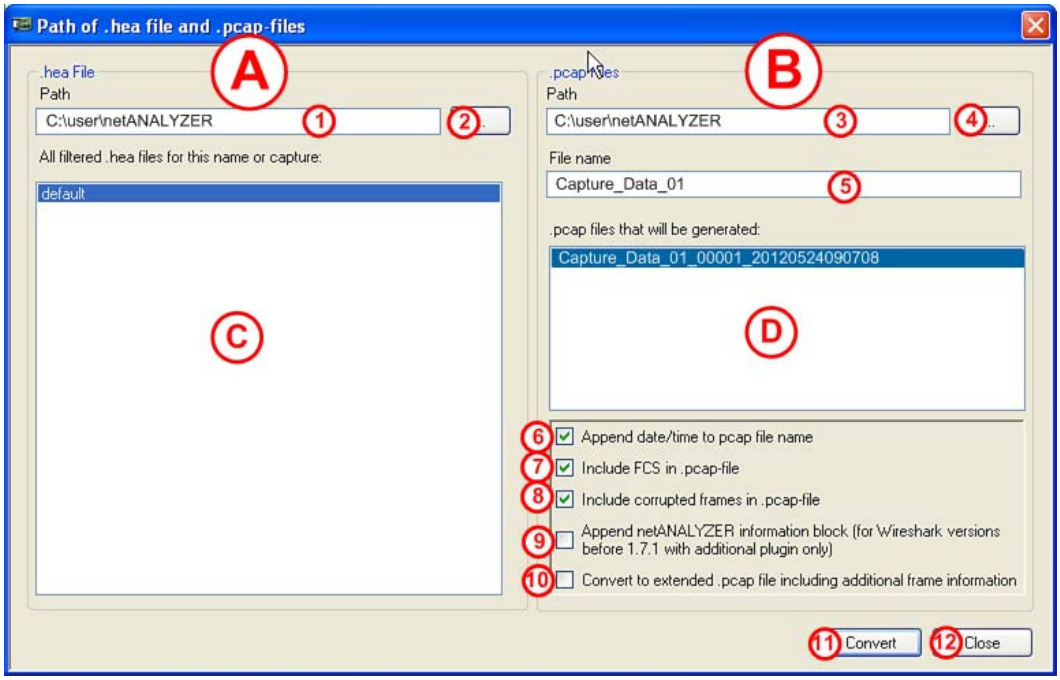


Abbildung 21: pcap-Konvertierung 1

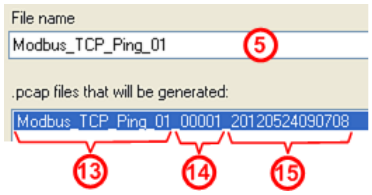
Das obige Fenster teilt sich in zwei Bereiche:

Fensterbereich (A)

Bedienelement	Erläuterung
Path (1)	Vom Bediener auszuwählender Pfad, aus welchem der netANALYZER die Binär-Datei (**.hea*) zur Konvertierung lesen soll. Die hier gemachten Einstellungen wirken sich auch auf die nächsten Datenaufzeichnungen aus. Die Einstellung unter **Settings > File Settings** wird damit verändert.
Schaltfläche (2)	Auswahlschaltfläche zur Auswahl des Quellverzeichnisses der .hea-Dateien.
All filtered .hea files for this name or capture (C)	Anzeigeliste der .hea-Dateien im ausgewähltem Verzeichnis

© Hilscher, 2008-2012

Fensterbereich B

Bedienelement	Erläuterung
Path 3	Der vom Bediener zu definierende Pfad, unter welchem die **netANALYZER**-Software die konvertierte WinPcap-Datei (**.pcap*) ablegen soll.
Schaltfläche 4	Auswahlschaltfläche zur Auswahl des Zielverzeichnis der .pcap-Dateien.
File name 5	Systematische Dateibezeichnung für die **.pcap*-Dateien. Die **netANALYZER**-Software vergibt zusätzlich für jede Datei noch eine fortlaufende Nummer im Dateinamen.
.pcap files that will be generated D	Vorschau der zu erzeugenden **.pcap*-Dateien. Dabei ist der Namensaufbau wie folgt:  13 der unter 5 ausgewählte Dateiname. 14 laufende Zählnummer 15 Zeitinformation, bestehend aus: yyyymmddhhmmss (Beginn der Aufzeichnung der hea-Datei, (nur wenn 6 der Haken gesetzt wurde.).
Append date/time to pcap file name 6	Ist der Haken gesetzt, werden Datum und Zeit im Dateinamen ergänzt.
Include FCS in .pcap-files 7	Checkbox ob die Ethernet-Prüfsumme mit in der PCAP-Datei enthalten sein soll oder nicht. (Einige Wireshark-Dissectoren unterstützen FCS nicht.) **Hinweis:** Wenn **Convert to extended .pcap file including additional frame information** angehakt ist, ist **Include FCS in .pcap-file** ausgegraut, da FCS dann immer in eine .pcap-Datei konvertiert wird. FCS = Frame Check Sequence (Ethernet-Prüfsumme) Nicht auswählbar, wenn Option 10 angehakt, jedoch aktiv.
Include corrupted frames in .pcap file 8	Ist diese Option aktiviert, werden auch fehlerhafte Frames in die .pcap-Datei übernommen. Ist die Option deaktiviert werden nur korrekte Telegramme in der .pcap-Datei gespeichert.
Append netANALYZER information block (for Wireshark versions before 1.7.1 with additional plug in only) 9	Die Option erfordert für Wireshark-Versionen < V1.7.1 die Installation des netANALYZER-Wireshark-Plugins. Fügt den netANALYZER-Info-Block nach dem Ethernet-Frame in die .pcap-Dateien ein. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen. **Hinweis:** Das .pcap-Dateiformat mit dem Info-Block nach dem Ethernet-Frame wird von Wireshark-Versionen ≥ 1.7.1 nicht mehr unterstützt. Nicht auswählbar, wenn Option 10 angehakt.
Convert to extended .pcap file including additional frame information 10	**Hinweis:** Wird dieser Haken gesetzt, kann das mit der netANALYZER-Software V1.4.x.x erzeugte erweiterte .pcap-Dateiformat nur in Wireshark-Versionen ab V1.7.1 geöffnet werden. Ab der Version der netANALYZER-Software V1.4.x.x kann ein erweitertes .pcap-Dateiformat erzeugt werden. Dabei befindet sich der „netANALYZER Info-Block“ in den 4 Bytes vor dem Ethernet-Frame. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen.
Convert 11	Die Konvertierung der Binär-Dateien ins WinPcap-Format wird gestartet.
Close 12	Sie schließen das Fenster ohne eine Konvertierung zu starten.

- ➢ Wählen Sie im Fensterbereich A die zu konvertierende Datei aus.
- ➢ Ergänzen Sie die notwendigen Einstellungen im Fensterbereich B.
- ➢ Klicken Sie auf die Schaltfläche **Convert** 11, um die Daten ins pcap-Format zu konvertieren.
- ➢ Nach Abschluss des Konvertierungsvorgangs schließt sich das Fenster.

© Hilscher, 2008-2012

➢ Öffnen Sie die Datei mit Wireshark.
Wenn das Programm Wireshark korrekt installiert ist, wird mittels eines Doppelklicks auf die .pcap-Datei diese mit Wireshark geöffnet.

➢ Es werden folgende Daten angezeigt:

➢ Doppelklick auf die konvertierte Datei (hier **Default_001.pcap**) oder starten Sie das Programm Wireshark, wählen Sie **File > Open** und dann die Datei aus.

➢ Das Programm Wireshark zeigt die Daten wie folgt an:

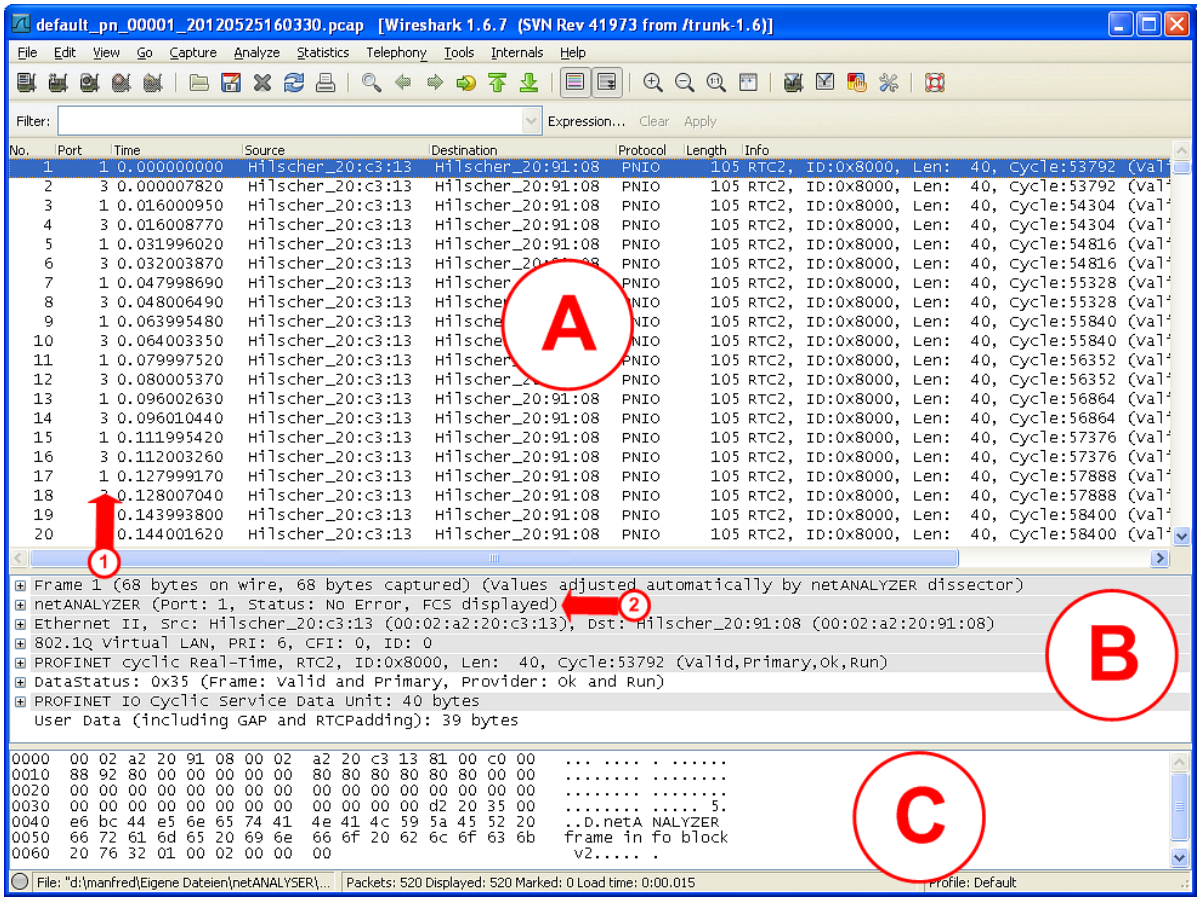

default_pn_00001_20120525160330.pcap [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Port Time Source Destination Protocol Length Info
1 1 0.000000000 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:53792 (Val
2 3 0.000007820 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:53792 (Val
3 1 0.016000950 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:54304 (Val
4 3 0.016008770 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:54304 (Val
5 1 0.031996020 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:54816 (Val
6 3 0.032003870 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:54816 (Val
7 1 0.047998690 Hilscher_20:c3:13 Hilscher PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:55328 (Val
8 3 0.048006490 Hilscher_20:c3:13 Hilsche NIO 105 RTC2, ID:0x8000, Len: 40, Cycle:55328 (Val
9 1 0.063995480 Hilscher_20:c3:13 Hilsche NIO 105 RTC2, ID:0x8000, Len: 40, Cycle:55840 (Val
10 3 0.064003350 Hilscher_20:c3:13 Hilsche NIO 105 RTC2, ID:0x8000, Len: 40, Cycle:55840 (Val
11 1 0.079997520 Hilscher_20:c3:13 Hilscher PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:56352 (Val
12 3 0.080005370 Hilscher_20:c3:13 Hilscher_2 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:56352 (Val
13 1 0.096002630 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:56864 (Val
14 3 0.096010440 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:56864 (Val
15 1 0.111995420 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:57376 (Val
16 3 0.112003260 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:57376 (Val
17 1 0.127999170 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:57888 (Val
18 3 0.128007040 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:57888 (Val
19 0.143993800 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:58400 (Val
20 0.144001620 Hilscher_20:c3:13 Hilscher_20:91:08 PNIO 105 RTC2, ID:0x8000, Len: 40, Cycle:58400 (Val
A
1
Frame 1 (68 bytes on wire, 68 bytes captured) (Values adjusted automatically by netANALYZER dissector)
netANALYZER (Port: 1, Status: No Error, FCS displayed)
2
Ethernet II, Src: Hilscher_20:c3:13 (00:02:a2:20:c3:13), Dst: Hilscher_20:91:08 (00:02:a2:20:91:08)
802.1Q Virtual LAN, PRI: 6, CFI: 0, ID: 0
PROFINET Cyclic Real-Time, RTC2, ID:0x8000, Len: 40, Cycle:53792 (Valid,Primary,Ok,Run)
DataStatus: 0x35 (Frame: Valid and Primary, Provider: Ok and Run)
PROFINET IO Cyclic Service Data Unit: 40 bytes
User Data (including GAP and RTCPadding): 39 bytes
B
0000 00 02 a2 20 91 08 00 02 a2 20 c3 13 81 00 c0 00 ... .
0010 88 92 80 00 00 00 00 00 80 80 80 80 80 80 00 00 ....
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 d2 20 35 00 .... 5.
0040 e6 bc 44 e5 6e 65 74 41 4e 41 4c 59 5a 45 52 20 ..D.netA NALYZER
0050 66 72 61 6d 65 20 69 6e 66 6f 20 62 6c 6f 63 6b frame in fo block
0060 20 76 32 01 00 02 00 00 00 v2..... .
C
File: "d:\manfred\Eigene Dateien\netANALYSER\... Packets: 520 Displayed: 520 Marked: 0 Load time: 0:00.015 Profile: Default

Abbildung 22: Telegrammdarstellung in Wireshark

© Hilscher, 2008-2012

Entsprechend der Filtereinstellung wurden nur Telegramme von der PC-Karte cifX zum Device 2 aufgezeichnet.

Ⓐ In diesem Fensterbereich werden alle aufgezeichneten Telegramme einzeln aufgelistet. In der Spalte **Port** ① sehen Sie die Portnummer der netANALYZER-Karte, an der das Telegramm aufgezeichnet wurde.

Ⓑ In diesem Fensterbereich werden die Daten des im Fensterbereich Ⓐ ausgewählten Telegramms auf Protokollebene dargestellt. In der Zeile 2 ② dieses Fensterbereichs sehen Sie die Portnummer der netANALYZER-Karte, an der das Telegramm aufgezeichnet wurde

Ⓒ In diesem Fensterbereich werden die Daten des ausgewählten Telegramms auf Byteebene dargestellt.

Hinweis: Im obigem Bild sind die einzelnen Telegramme 2 mal aufgelistet. Die Ursache liegt im Schaltungsaufbau aus 4.1 und der gewählten Filtereinstellung, da die netANALYZER-Karte die Daten an jedem TAP aufzeichnet, und die gefilterten Telegramme an beiden Port's vorbeikommen. Hier ist somit auch die Laufzeit durch den Device 1 zu ersehen.

© Hilscher, 2008-2012

4.4 Netzlast-Analyse vorbereiten und durchführen

Es sollen die Netzlast, ausgelöst durch die PC-Karte cifX, analysiert werden. Es soll analysiert werden, wie groß der Anteil der PROFINET-Telegramme zu anderen Telegrammen ist. Es soll das Netzwerk-Anlaufverhalten untersucht werden.

Voraussetzungen:

- Der Hardware-Aufbau, wie in *Hardware-Aufbau* auf Seite 16 beschrieben, muss erstellt sein,
- die Einstellungen für die PC-Karte cifX müssen erfolgt sein,
- es muss ein Datenaustausch zwischen der PC-Karte cifX und den Devices erfolgen.

4.4.1 Netzlast-Analyse vorbereiten

Es müssen die Filterkriterien ermittelt und anschließend eingestellt werden.

➢ Machen Sie eine kurze Datenaufzeichnung an einem laufenden PROFINET Netzwerk.

➢ Sehen Sie sich ein Standard PROFINET-Telegramm an.

➢ Dieser Datensatz sollte wie folgt aussehen:

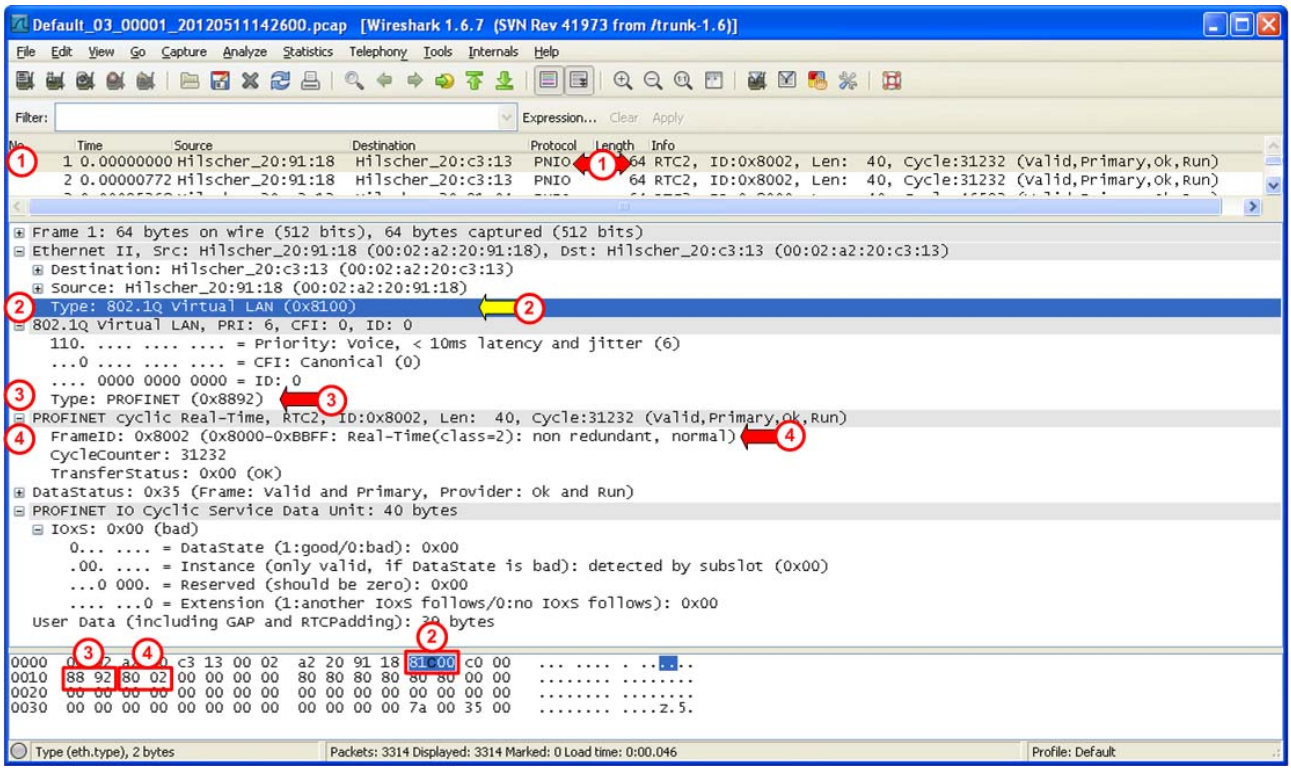

Default_03_00001_20120511142600.pcap [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
1 0.00000000 Hilscher_20:91:18 Hilscher_20:c3:13 PNIO 64 RTC2, ID:0x8002, Len: 40, Cycle:31232 (Valid,Primary,Ok,Run)
2 0.00000772 Hilscher_20:91:18 Hilscher_20:c3:13 PNIO 64 RTC2, ID:0x8002, Len: 40, Cycle:31232 (Valid,Primary,Ok,Run)
Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
Ethernet II, Src: Hilscher_20:91:18 (00:02:a2:20:91:18), Dst: Hilscher_20:c3:13 (00:02:a2:20:c3:13)
Destination: Hilscher_20:c3:13 (00:02:a2:20:c3:13)
Source: Hilscher_20:91:18 (00:02:a2:20:91:18)
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 6, CFI: 0, ID: 0
110. .... = Priority: Voice, < 10ms latency and jitter (6)
...0 .... = CFI: Canonical (0)
.... 0000 0000 0000 = ID: 0
Type: PROFINET (0x8892)
PROFINET cyclic Real-Time, RTC2, ID:0x8002, Len: 40, Cycle:31232 (Valid,Primary,Ok,Run)
FrameID: 0x8002 (0x8000-0xBBFF: Real-Time(class=2): non redundant, normal)
CycleCounter: 31232
TransferStatus: 0x00 (OK)
DataStatus: 0x35 (Frame: Valid and Primary, Provider: Ok and Run)
PROFINET IO Cyclic Service Data Unit: 40 bytes
IOxS: 0x00 (bad)
0... .... = DataState (1:good/0:bad): 0x00
.00. .... = Instance (only valid, if DataState is bad): detected by subslot (0x00)
...0 000. = Reserved (should be zero): 0x00
....0 = Extension (1:another IOxS follows/0:no IOxS follows): 0x00
User Data (including GAP and RTCPadding): 30 bytes
0000 00 02 a2 20 91 18 81 00 c0 00
0010 88 92 80 02 00 00 00 00 80 80 80 80 80 80 00 00
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 7a 00 35 00
Type (eth.type), 2 bytes
Packets: 3314 Displayed: 3314 Marked: 0 Load time: 0:00.046
Profile: Default

Abbildung 23: Standard PROFINET Datensatz

In der obigen Abbildung sind die relevanten Filterdaten von ① bis ④ markiert.

① Ein Standard PROFINET Protokoll-Telegramm.

② Die virtual LAN Kennung (0x **81 00**).

③ Die PROFINET Kennung 0x **88 92**).

④ Die Frame ID Kennung (0x**80 02**).

➢ Konfigurieren Sie mit den obigen Daten ein *Extended Software Filter*.

© Hilscher, 2008-2012

4.4.2 Filter einstellen

➢ Hardware-Filter ausschalten

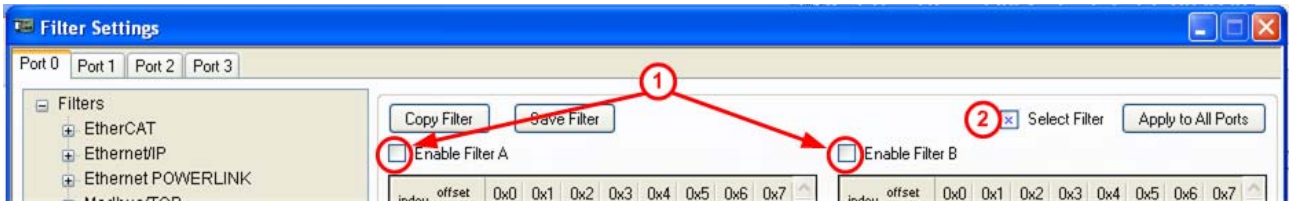


Abbildung 24: Hardware-Filter ausschalten

Hinweis: Die eingestellten Hardware (Standard-Filter) wirken additiv zu dem *Extended Software Filter*. Aus diesem Grunde entfernen wir die Haken bei **Enable Filter** ① aus dem Hardware-Filter, oder den Haken bei **Select Filter** ②.

➢ Softwarefilter einstellen.

➢ Zur Konfiguration der *Extended Software Filter* gehen Sie wie folgt vor:

1. Wählen Sie im netANALYZER Hauptfenster **Settings > Extended Software Filter Settings**.

Es öffnet sich folgendes Konfigurationsfenster:

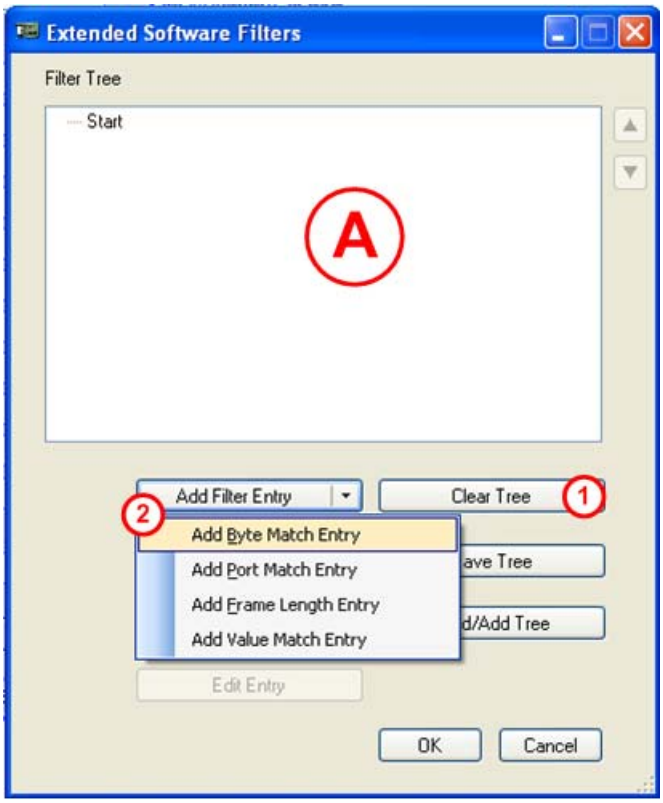


Abbildung 25: Extended Software Filter erstellen (1)

2. Erstellen Sie die Filtereinträge. Dazu gehen Sie wie folgt vor:

➢ Sollte im Fensterbereich Ⓐ mehr stehen als in der obigen Abbildung dargestellt ist, löschen Sie die Einträge mit **Clear Tree** ①.

➢ Öffnen Sie das Auswahlmenü unter der Schaltfläche **Add Filter Entry** ② und wählen den Eintrag **Add Byte Match Entry** aus.

Es öffnet sich folgendes Konfigurationsfenster:

© Hilscher, 2008-2012

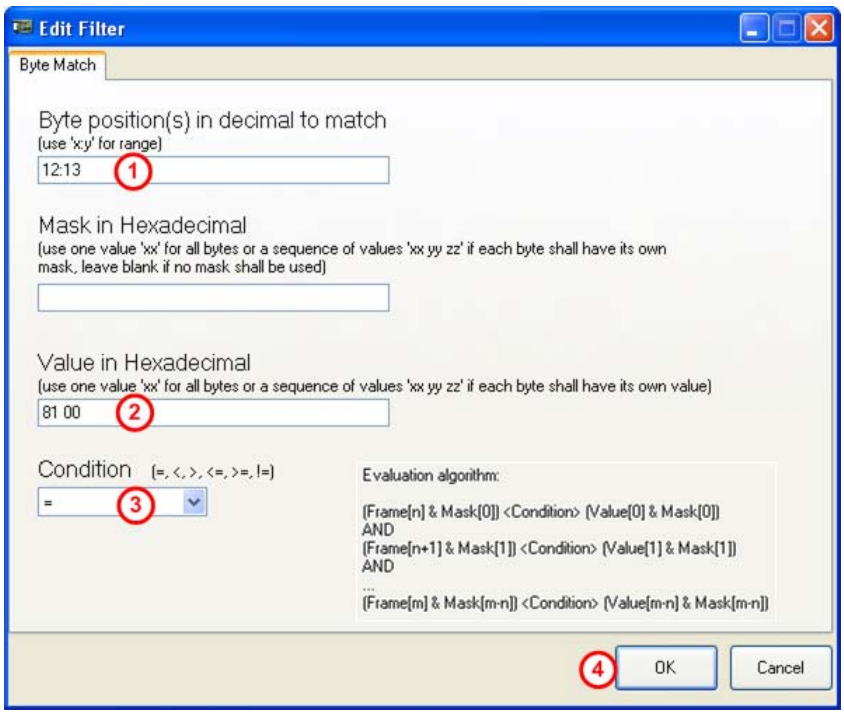

Edit Filter
Byte Match
Byte position(s) in decimal to match
(use 'x:y' for range)
12:13
1
Mask in Hexadecimal
(use one value 'xx' for all bytes or a sequence of values 'xx yy zz' if each byte shall have its own mask, leave blank if no mask shall be used)
Value in Hexadecimal
(use one value 'xx' for all bytes or a sequence of values 'xx yy zz' if each byte shall have its own value)
81 00
2
Condition (=, <, >, <=, >=, !=)
=
3
Evaluation algorithm:
(Frame[n] & Mask[0]) <Condition> (Value[0] & Mask[0])
AND
(Frame[n+1] & Mask[1]) <Condition> (Value[1] & Mask[1])
AND
...
(Frame[m] & Mask[m-n]) <Condition> (Value[m-n] & Mask[m-n])
4
OK
Cancel

Abbildung 26: Extended Software Filter erstellen (2)

- Tragen Sie hier die Filterdaten ein, die Sie in der *Abbildung 23* unter dem Eintrag ② ermittelt haben:
  In der obigen Abbildung unter ① die Byte Position (hier 12:13; **Achtung, die Bytezählung beginnt bei „0“**), unter ② den Dateninhalt dieser Position (hier 81 00) und unter ③ die Vergleichsbedingung (hier „=“). Klicken Sie anschließend **OK** ④.
- Das *Extended Software Filter* sollte jetzt wie folgt aussehen:

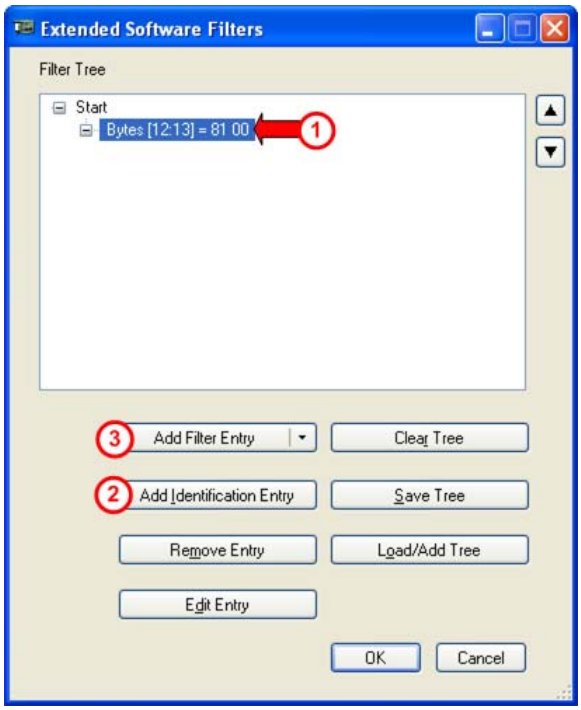


Abbildung 27: Extended Software Filter nach 1. Eintrag

© Hilscher, 2008-2012

Zur PROFINET Identifikation gehen Sie wie folgt vor:

- Ermitteln Sie aus der Abbildung 23 Eintrag (3), die Informationen für die PROFINET-Kennung.
- Markieren Sie den Eintrag (1) der obigen Filterabbildung und fügen dann mit **Add Filter Entry** (2) den Eintrag „Bytes [16:17] = 88 92“ (3) wie für den Eintrag (1) beschrieben hinzu.

Hinweis: Hierdurch wird eine UND-Verknüpfung der Filterbedingung erzeugt. Hätten Sie den Eintrag Start (der obigen Abbildung) markiert, würden die beiden Einträge ODER verknüpft.

Jetzt sollte Ihr Filter wie folgt dargestellt aussehen.

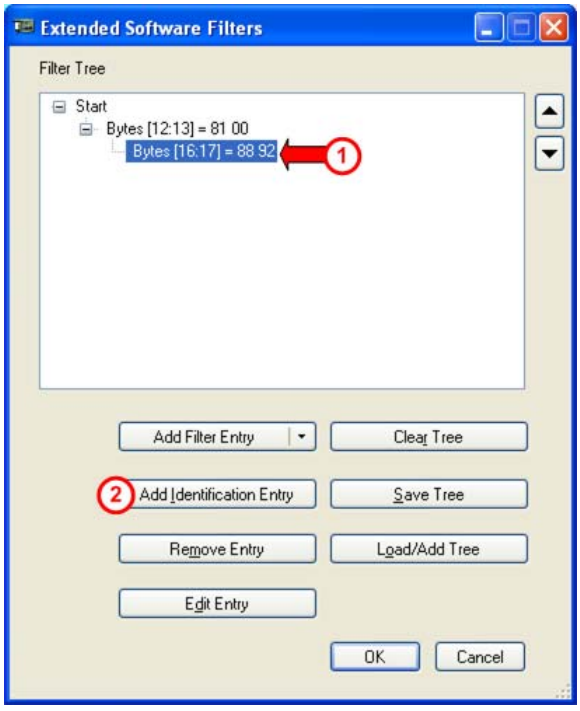


Abbildung 28: Extended Software Filter nach 2. Eintrag

Damit Sie in der Netload Analysis Grafik eine Kurve dargestellt bekommen, müssen noch einen Identifikations-Eintrag hinzufügen.

- Dazu klicken Sie den in der obigen Filterdarstellung den mit (1) markierten Eintrag an. Klicken Sie anschließend **Add Identification Entry**.
- In dem sich dann öffnenden Fenster tragen Sie einen Identifikationsnamen ein. Hier wurde der Name „PROFINET“ eingetragen.

Hinweis: Treten bei der Analyse noch andere Datensätze auf, die nicht den Filterbedingungen entsprechen, werden diese mit der Kennung **Other** erfasst.

© Hilscher, 2008-2012

Damit sieht das Filterfenster jetzt wie folgt aus.

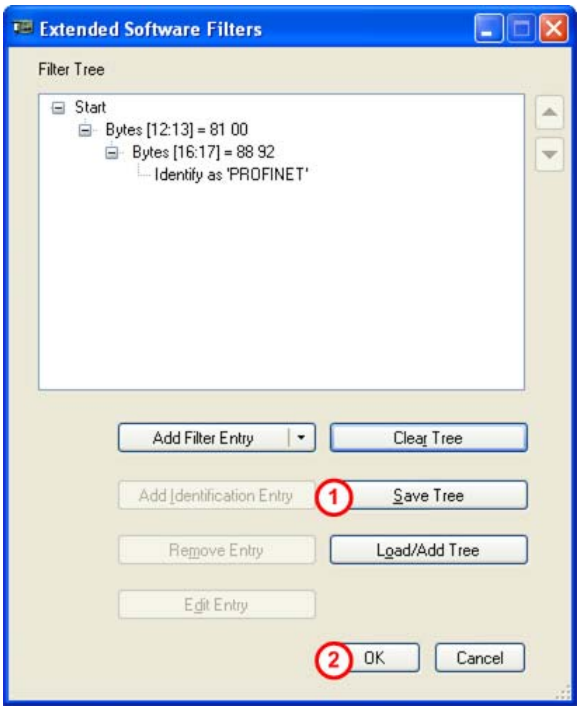


Abbildung 29: Extended Software Filter nach 3. Eintrag

- Speichern Sie die Filtereinstellungen für spätere Anwendungen mit **Save Tree** (1) und verlassen Sie das Filterfenster mit **OK** (2).

Sie gelangen zurück in das Hauptfenster des netANALYZERs.

Nehmen Sie hier folgende Einstellungen vor:

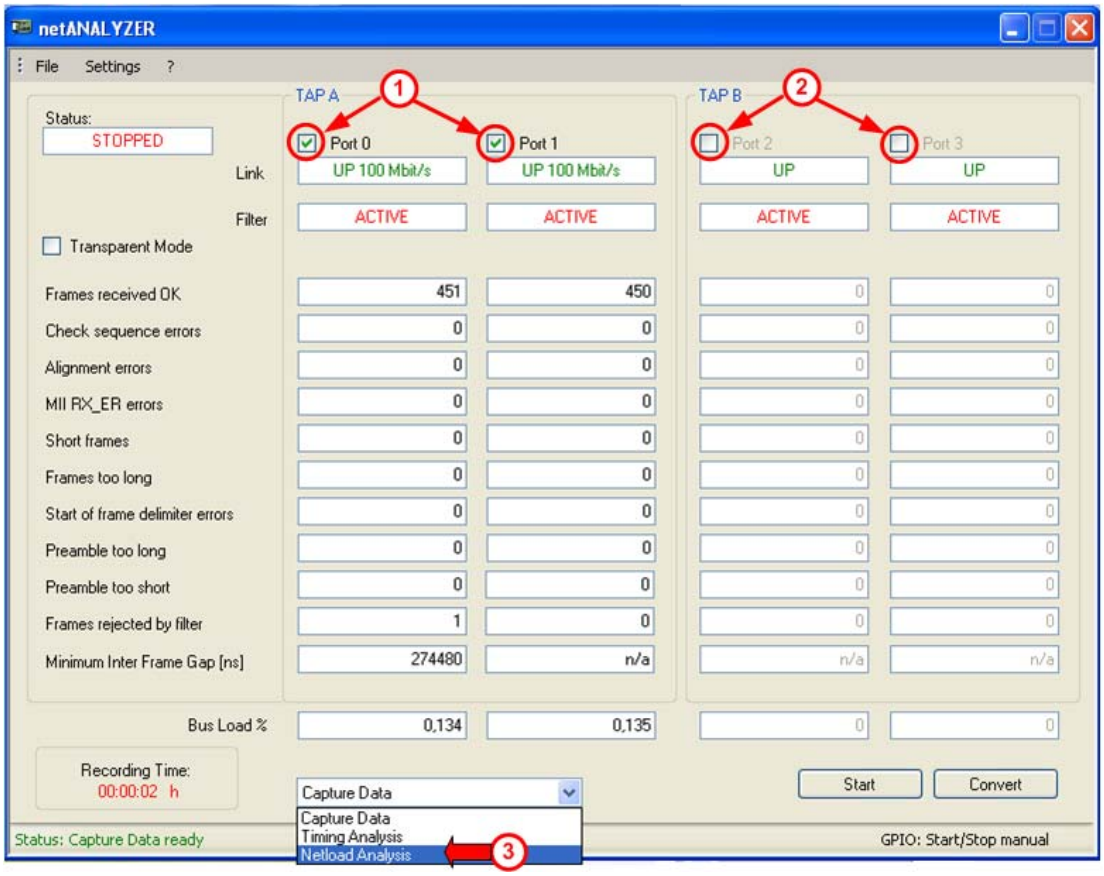


Abbildung 30: netANALYZER Hauptfenster PROFINET Netload Analyse

© Hilscher, 2008-2012

- Setzen Sie den Haken bei TAP A für Port 0 und Port 1 (1). Dieses ist erforderlich, da wegen der Auto Cross Over Funktionalität der Ethernetanschlüsse nicht vorhersehbar ist, über welchen Port die Kommunikation startet.
- Entfernen Sie ggf. die Haken bei TAP B (2), damit die Telegramme nicht doppelt aufgezeichnet werden.

4.4.3 Netzlast-Messung durchführen

- Wählen Sie für die Analyse unter **Netload Analysis** (3) aus.
- Es öffnet sich das Netload Analysis Fenster.
- Öffnen Sie die Ethernetverbindung am CH 0 des Device 1 der Abbildung 5 um sie nach dem Start der Analyseaufzeichnung wieder schließen zu können, damit die nicht PROFINET Frames bei Verbindungsaufbau erfasst werden können.
- Wählen Sie das Hauptfenster des netANALYZER an.
- Klicken Sie **Start**.
- Die Datenaufzeichnung beginnt.
- Schließen Sie das Kabel am CH 0 des Devices wieder an.
- Stoppen Sie nach einiger Zeit der Aufzeichnung mit **Stop** im Hauptfenster des netANALYZERs.
- Im Netload Analysis Fenster sehen Sie jetzt etwa folgende Informationen:

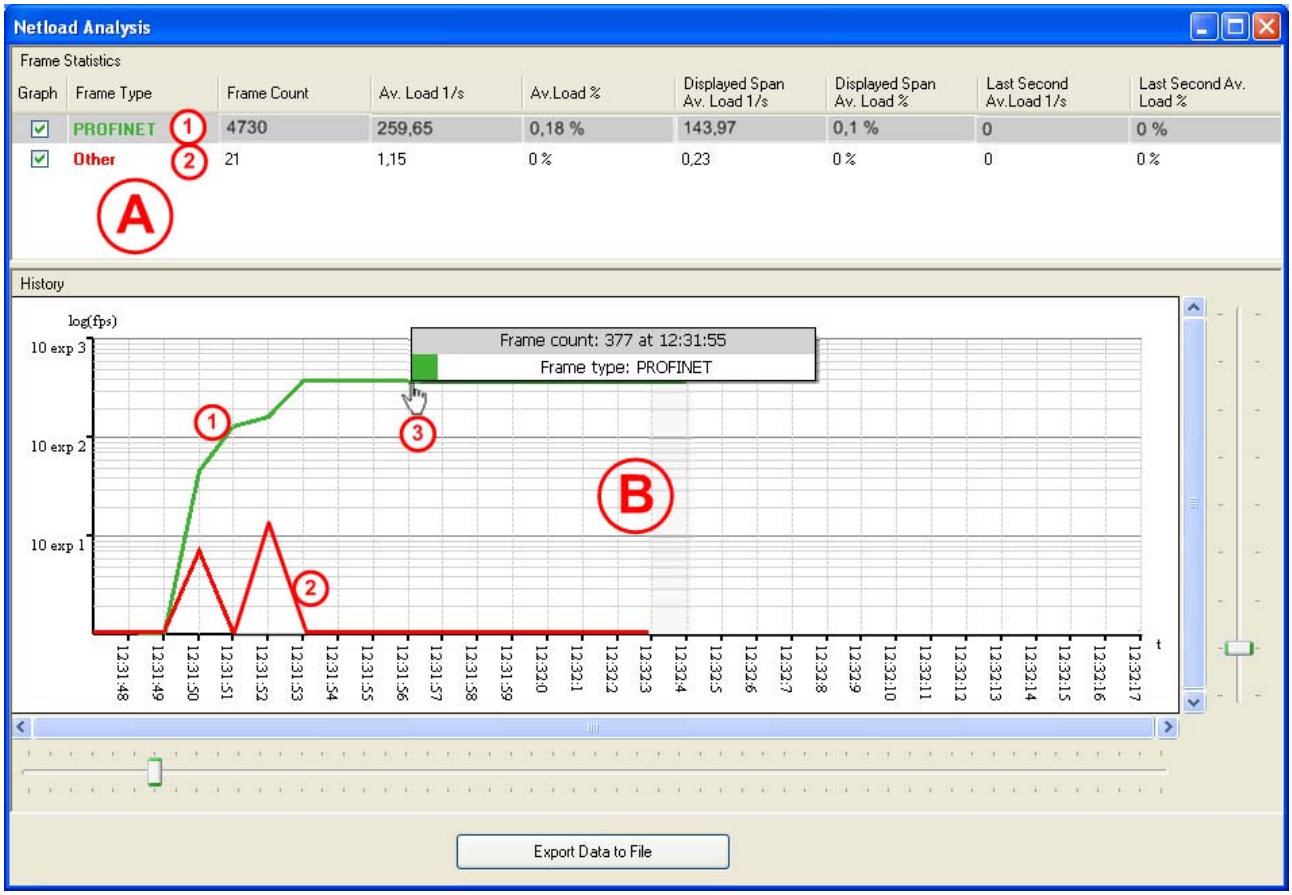


Abbildung 31: Netload Analyse für PROFINET Anlaufphase

© Hilscher, 2008-2012

Zeile ① im Fensterbereich Ⓐ korrespondiert mit der Linie ① im Fensterbereich Ⓑ.

Zeile ② im Fensterbereich Ⓐ korrespondiert mit der Linie ② im Fensterbereich Ⓑ.

Neben der in den Filtereinstellungen benannten Selektion wird automatisch der „Rest“, der nicht den Selektionsbedingungen des Filters entspricht, als **Other** in der Grafik dargestellt.

Im Fensterbereich Ⓐ sehen Sie die numerischen Werte der Aufzeichnung. Klicken Sie hier mit der rechten Maustaste auf einen Frame Type, dann können Sie im Kontextmenü die Kurvenfarbe, Linientyp und Liniendicke auswählen, wie diese im Fensterbereich Ⓑ dargestellt werden sollen.

Klicken Sie im Fensterbereich Ⓑ auf die rechte Maustaste, dann können Sie die Y-Skalierung z.B. von linear auf logarithmisch umstellen.

Fahren Sie mit der Maus im Fensterbereich Ⓑ entlang einer Kurve, dann werden Ihnen die numerischen Messwerte für diese Messsekunde angezeigt ③.

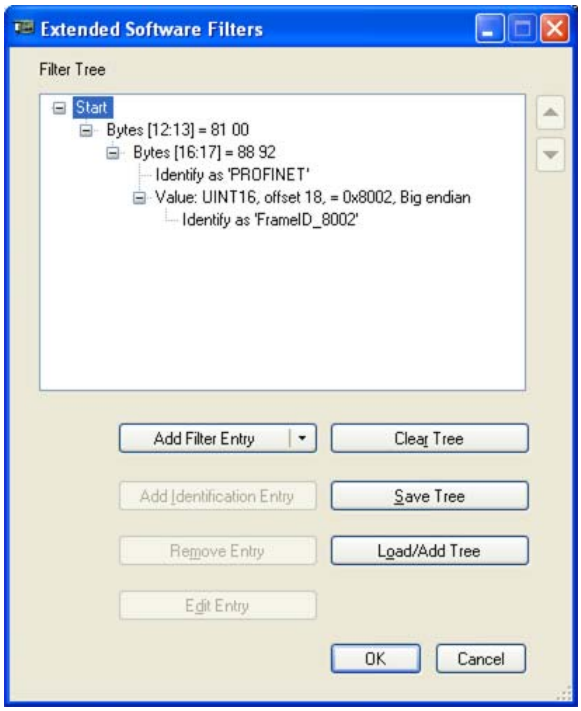


Abbildung 32: Extended Software Filter mit FrameID

Mit folgender **erweiterter Extended Software Filtereinstellung**, in der noch nach einer bestimmten FrameID gefiltert wird, bekommt man folgendes Analysis Bild für die Anlaufphase des PROFINET Netzwerkes:

© Hilscher, 2008-2012

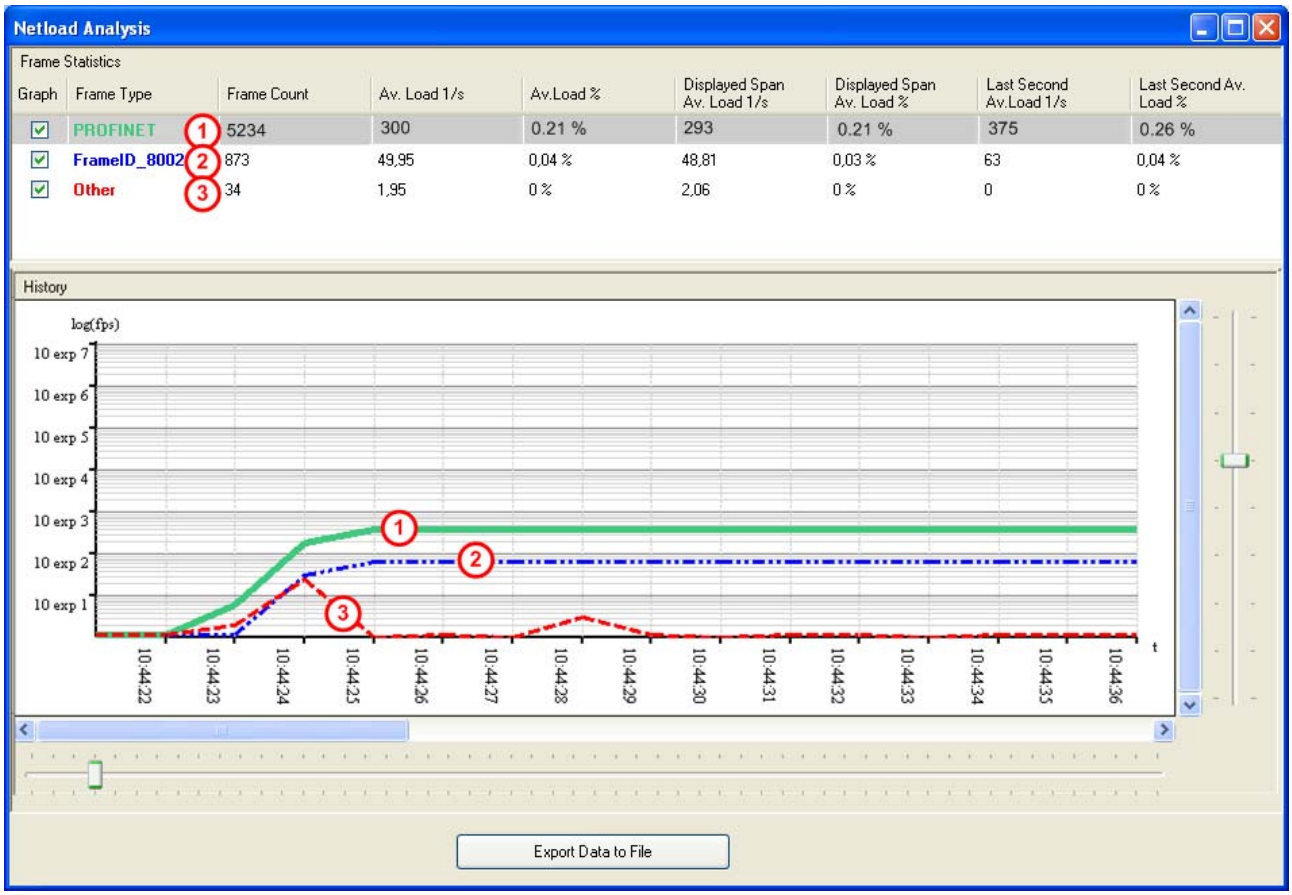


Abbildung 33: Netload Analyse für PROFINET Anlaufphase mit FrameID 8002

© Hilscher, 2008-2012

5 EtherCAT Analyse

Beispielhaft werden hier folgende Messungen durchgeführt:

- Messung der Zykluszeit des Masters,
- Messung der Telegrammdurchlaufzeit durch Slave 1,
- Messung der Ringdurchlaufzeit der Telegramme.

5.1 Hardware-Aufbau

Für diese Beispielmessung wird folgender Hardware-Aufbau benötigt.

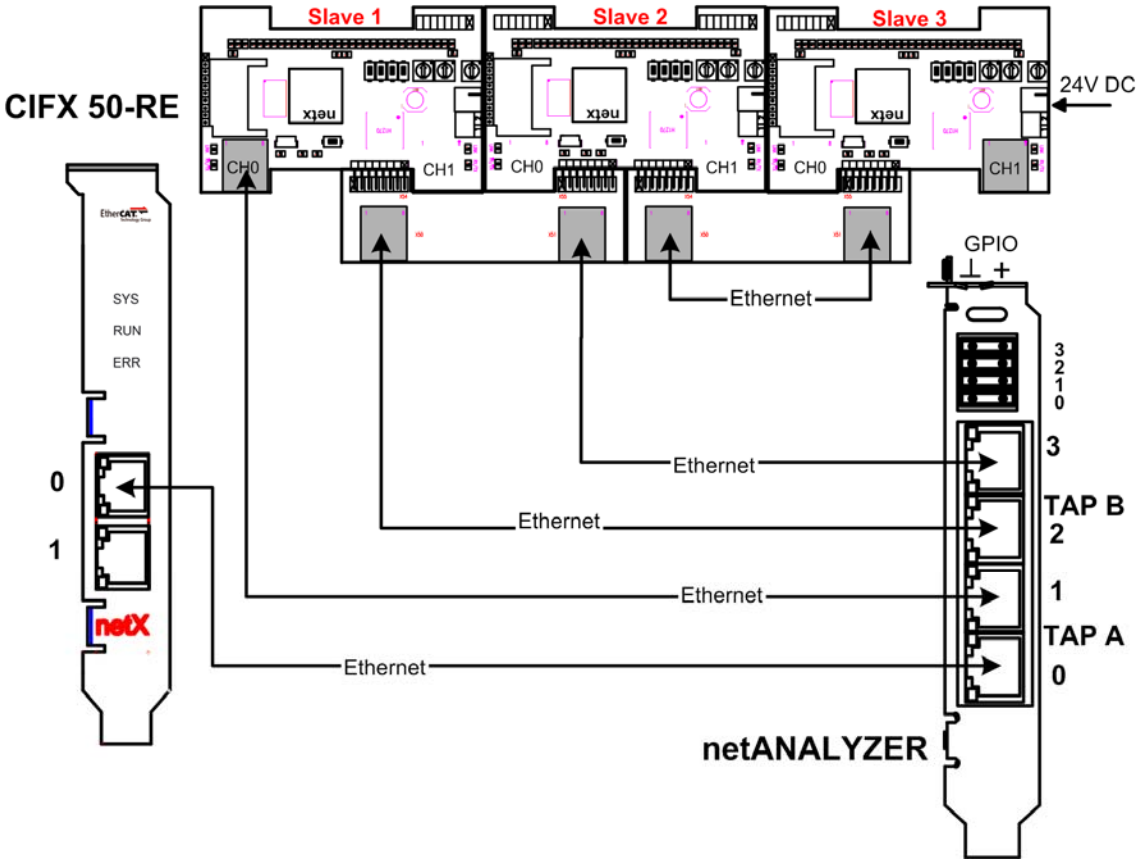


Abbildung 34: EtherCAT Hardware-Aufbau

Achtung! Es ist wichtig, dass der Ethernetanschluss **CH0 der PC-Karte cifX** mit dem **CH0 Ethernetanschluss auf dem NXIO 50-Board** verbunden wird.

Hinweis: Die Einstellungen für die PC-Karte cifX und die NXIO 50 Boards müssen entsprechend Abschnitt 6.3 des *Benutzerhandbuch Real-Time-Ethernet-Kit - Kommunikationssysteme für Real-Time-Ethernet Installation, Bedienung und Konfiguration* vorgenommen worden sein.

© Hilscher, 2008-2012

5.2 Zeitmessungen vorbereiten und durchführen

Hinweis: Die PC-Karte cifX und die NXIO-Boards verfügen über eine Autocrossover-Funktionalität. Daher ist ein vertauschen der Kabel am netANALYZER am TAP A (Port 0 und Port 1) sowie am TAP B (Port 2 und Port 3) ohne Bedeutung. Somit sind auch bei der Anzeige der Analysewerte die Portbezeichnungen 0/1 bzw. 2/3 als vertauschbar zu betrachten.
An der cifX ist jedoch unbedingt der Port 0 zu verwenden!

Hinweis: Hier sind nur die für diesen Messaufbau unmittelbar erforderlichen Einstellungen des netANALYZERs beschrieben. Detaillierte Informationen über die Einstell- und Aufzeichnungsmöglichkeiten der Software entnehmen Sie bitte der Dokumentation *Benutzerhandbuch netANALYZER Installation, Bedienung und Hardware-Beschreibung*.

5.2.1 Zeitmessung vorbereiten

Es soll die Zykluszeit der Telegramme der PC-Karte cifX zum Slave 1 und die Gerätedurchlaufzeit von Slave 1, sowie die Ringdurchlaufzeit gemessen werden.

➢ Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

⇘ Sie gelangen ins das Hauptfenster des netANALYZERs.

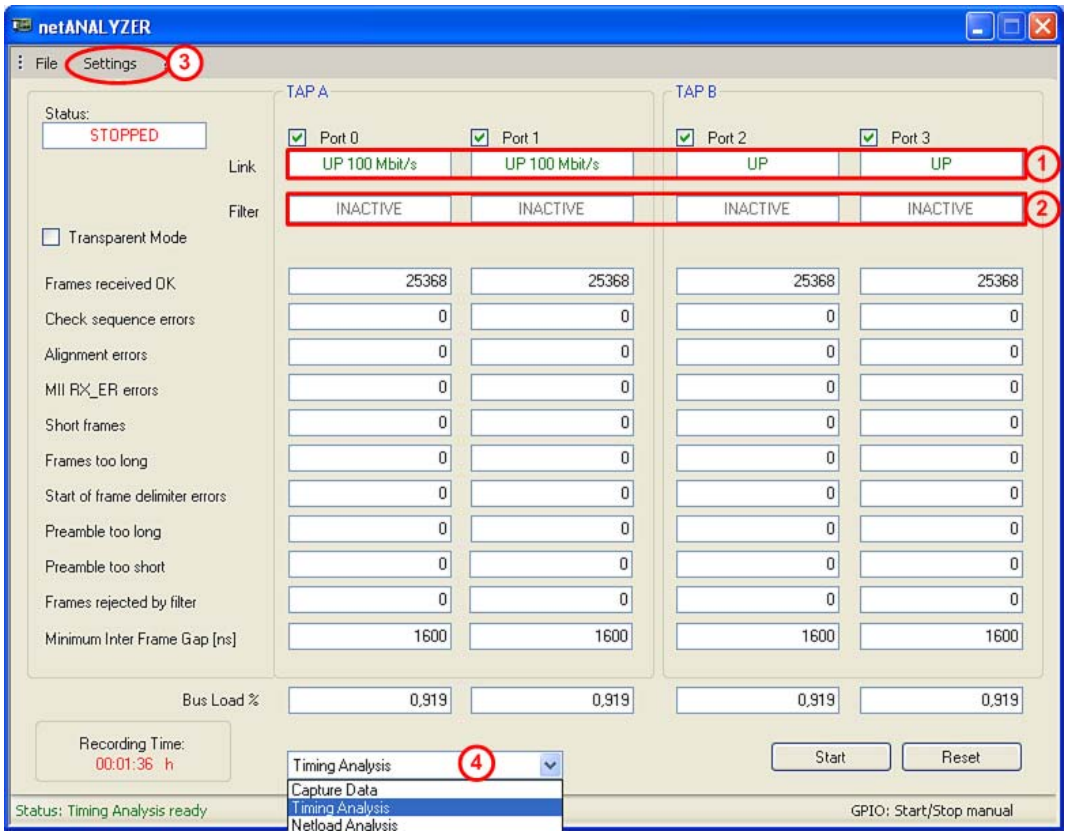


Abbildung 35: netANALYZER Hauptfenster

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 42 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP mit Datenrate** oder bei älteren netANALYZER-Karten bei TAP B nur mit **UP** gekennzeichnet.

© Hilscher, 2008-2012

5.2.2 Filter einstellen

➢ Nehmen Sie unter **Settings > Filter Settings** ③ folgende Einstellungen vor:

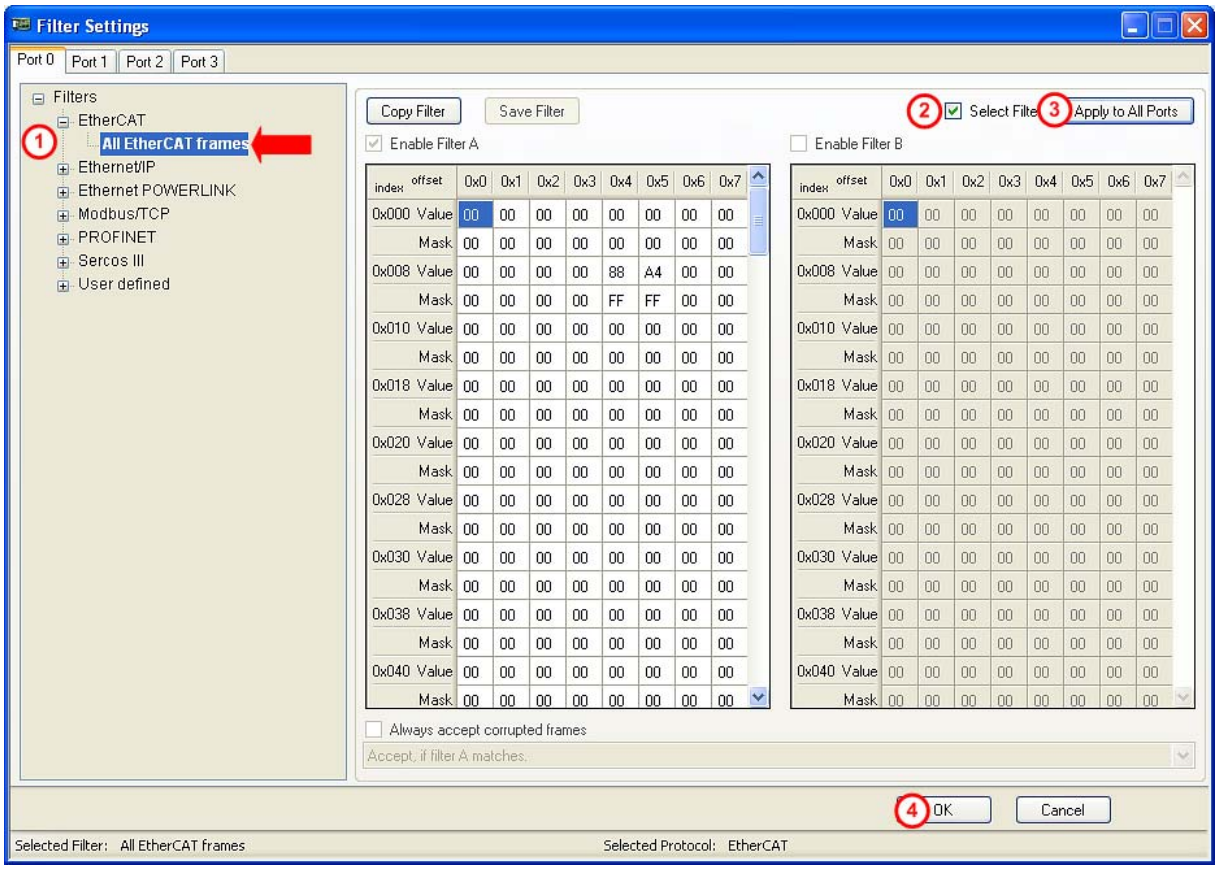


Abbildung 36: netANALYZER Filterfenster

➢ Wählen Sie **Filters > EtherCAT > All EtherCAT frames** ①.

➢ Klicken Sie **Select Filter** ②.

➢ Klicken Sie **Apply to All Ports** ③.

➢ Kontrollieren Sie, ob der ausgewählte Filter auf alle Ports angewendet wird.

➢ Verlassen Sie die Filtereinstellungen mit **OK** ④.

↬ Sie gelangen zurück ins Hauptfenster des netANALYZERs.

➢ Wählen Sie im netANALYZER Hauptfenster **Timing Analysis** ④.

↬ Es öffnet sich im Vordergrund das Fenster zur grafischen Darstellung der Zeitanalyse (Timing Analysis).

© Hilscher, 2008-2012

Abbildung 37: netANALYZER Timing-Analyse-Fenster

Das Timing Analysis-Fenster unterteilt sich in 4 Unterfenster, die wiederum 2 Teilfenster (Histogramm und Historie) beinhalten. Im weiteren Verlauf dieses Messaufbaus wird in der Regel immer nur ein Unterfenster angesprochen.

Die Größe der Einzelfenster können Sie durch ziehen des Kreuzungspunktes der Fensterteilungslinien verändern.

Sie können sich auch nur das Historie- oder Histogramm-Fenster anzeigen lassen. Dieses können Sie im Haupt-Fenster des netANALYZERs unter **Settings > Analysis Configuration** einstellen.

5.2.3 Einstellungen in den Timing-Analysefenstern

Achten Sie darauf, dass in allen Unterfenstern zunächst **Auto Scale** ① eingestellt ist.

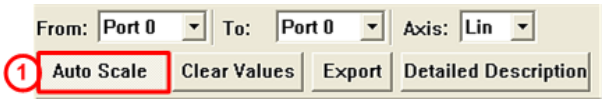


Abbildung 38: netANALYZER Timing-Auto-Scale

Damit stellen Sie sicher, dass (wenn Telegramme detektiert werden) diese auch als Balken sichtbar sind und nicht außerhalb des Zeitstrahls liegen. (Achtung: Der Zeitstrahl geht in dieser Darstellung senkrecht nach oben.)

➢ Stellen Sie die From / To - Bedingungen für jedes Teilfenster wie folgt ein:

Hinweis: Wegen der Autocrossover-Funktionalität. der Ports der netANALYZER-Karte können bei Ihrem Testaufbau. die Telegramme ggf. auch über die entsprechenden korrespondierenden Port laufen. Passen Sie die Ports entsprechend Ihres Aufbaus an.

© Hilscher, 2008-2012

5.2.3.1 Einstellungen für Analysefenster A

Zur Messung der Zykluszeit der Telegramme der PC-Karte cifX zum Slave 1

➢ Nehmen Sie im Fenster A folgende Einstellungen vor:

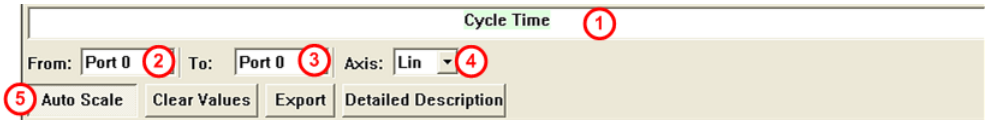


Abbildung 39: Timing-Analysefenster A, EtherCAT Zykluszeit

➢ In dieser Zeile können Sie eine beliebige Bezeichnung für diese Messung eingeben. Geben Sie hier **Zykluszeit** (1) ein.

➢ Unter **From:** wählen Sie **Port 0** (2) aus.

➢ Unter **To:** wählen Sie **Port 0** (3) aus.
Mit dieser Einstellung wird die Zykluszeit gemessen.

➢ Hier kann die Skalierung der X-Achse (4) im Teilfenster „**A 1**“ zwischen linear und logarithmisch umgeschaltet werden.

➢ Achten Sie darauf, dass für die Zeitachsen **Auto Scale** (5) eingestellt ist.

5.2.3.2 Einstellungen für Analysefenster B

Zur Messung der Ringdurchlaufzeit / Zykluszeit

➢ Nehmen Sie im Fenster B folgende Einstellungen vor:

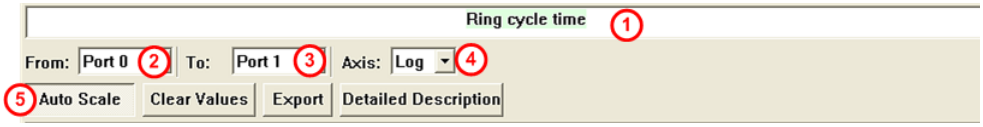


Abbildung 40: Timing-Analysefenster B, EtherCAT Ringdurchlaufzeit (1)

➢ Unter **From:** wählen Sie **Port 0** (2) aus

➢ Unter **To:** wählen Sie **Port 1** (3) aus.
Mit dieser Einstellung wird die Zeit zwischen dem Auftreten des Telegramms am Port 0 und dem Auftreten am Port 1 gemessen. Dieses kann die Ringdurchlaufzeit sein, oder die Zykluszeit minus Ringdurchlaufzeit. Dieses kann erst nach erfolgter Messung interpretiert werden (siehe auch Einstellungen für Fenster C). Diese mögliche Mehrdeutigkeit kommt von der Autocrossover-Funktionalität der PC-Karte cifX und den NXIO-Boards.

© Hilscher, 2008-2012

5.2.3.3 Einstellungen für Analysefenster C

Zur Messung der Ringdurchlaufzeit / Zykluszeit:

➢ Nehmen Sie im Fenster C folgende Einstellungen vor:

Abbildung 41: Timing-Analysefenster C, EtherCAT Ringdurchlaufzeit (2)

➢ Unter **From:** wählen Sie **Port 1** (2) aus.

➢ Unter **To:** wählen Sie **Port 0** (3) aus.
Mit dieser Einstellung wird die Zeit zwischen dem Auftreten des Telegramms am Port 0 und dem Auftreten am Port 1 gemessen. Dieses kann die Ringdurchlaufzeit sein, oder die Zykluszeit minus Ringdurchlaufzeit. Dieses kann erst nach erfolgter Messung interpretiert werden (siehe auch Einstellungen für Fenster B). Diese mögliche Mehrdeutigkeit kommt von der Autocrossover-Funktionalität der PC-Karte cifX und den NXIO-Boards.

5.2.3.4 Einstellungen für Analysefenster D

Zur Messung der Signaldurchlaufzeit Slave 1

➢ Nehmen Sie im Fenster D folgende Einstellungen vor:

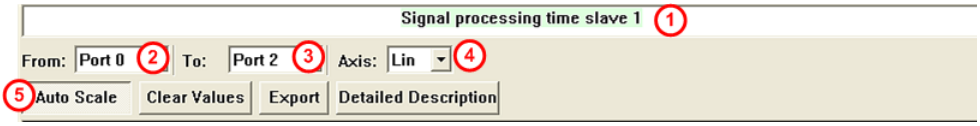


Abbildung 42: Timing-Analysefenster D, EtherCAT Ringdurchlaufzeit (2)

➢ Unter **From:** wählen Sie **Port 0** (2) aus (ggf. **Port 1**).

➢ Unter **To:** wählen Sie **Port 2** (3) aus (ggf. **Port 3**).
Mit einem der beiden Einstellpaare wird die Signaldurchlaufzeit durch den Slave 1 ermittelt. Wird hier Port 2 und Port 3 vertauscht (von der Crossover-Funktionalität des TAP abhängig) wird eine Größe um die Zykluszeit ermittelt.

5.2.4 Messung durchführen

➢ Klicken Sie im Hauptfenster des netANALYZERS

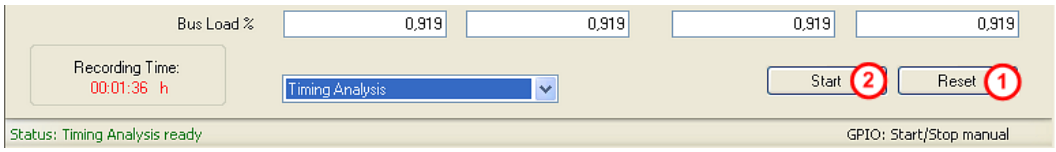


Abbildung 43: netANALYZER Start / Stopp Analyse

➢ Klicken Sie **Reset** (1). Damit werden die bisher aufgezeichneten Zeit-Daten gelöscht.

➢ Klicken Sie **Start** (2) um die Analyse zu starten.

↬ Die Schaltfläche **Start** wird zur Schaltfläche **Stop**.

➢ Warten Sie die Zeit, in der Sie Telegramme auswerten möchten.

➢ Klicken Sie **Stop**.

© Hilscher, 2008-2012

5.2.4.1 Messergebnis Fenster A: Zykluszeit

Sind From- und Stop-Port identisch, wird immer die Zykluszeit gemessen, unabhängig davon, ob im Datenweg vom Master zu den Slaves oder im Datenweg von den Slaves zum Master gemessen wird. Im Datenweg der Slaves zum Master kann aber der Jitter erhöht sein.

➭ Im Fenster A des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

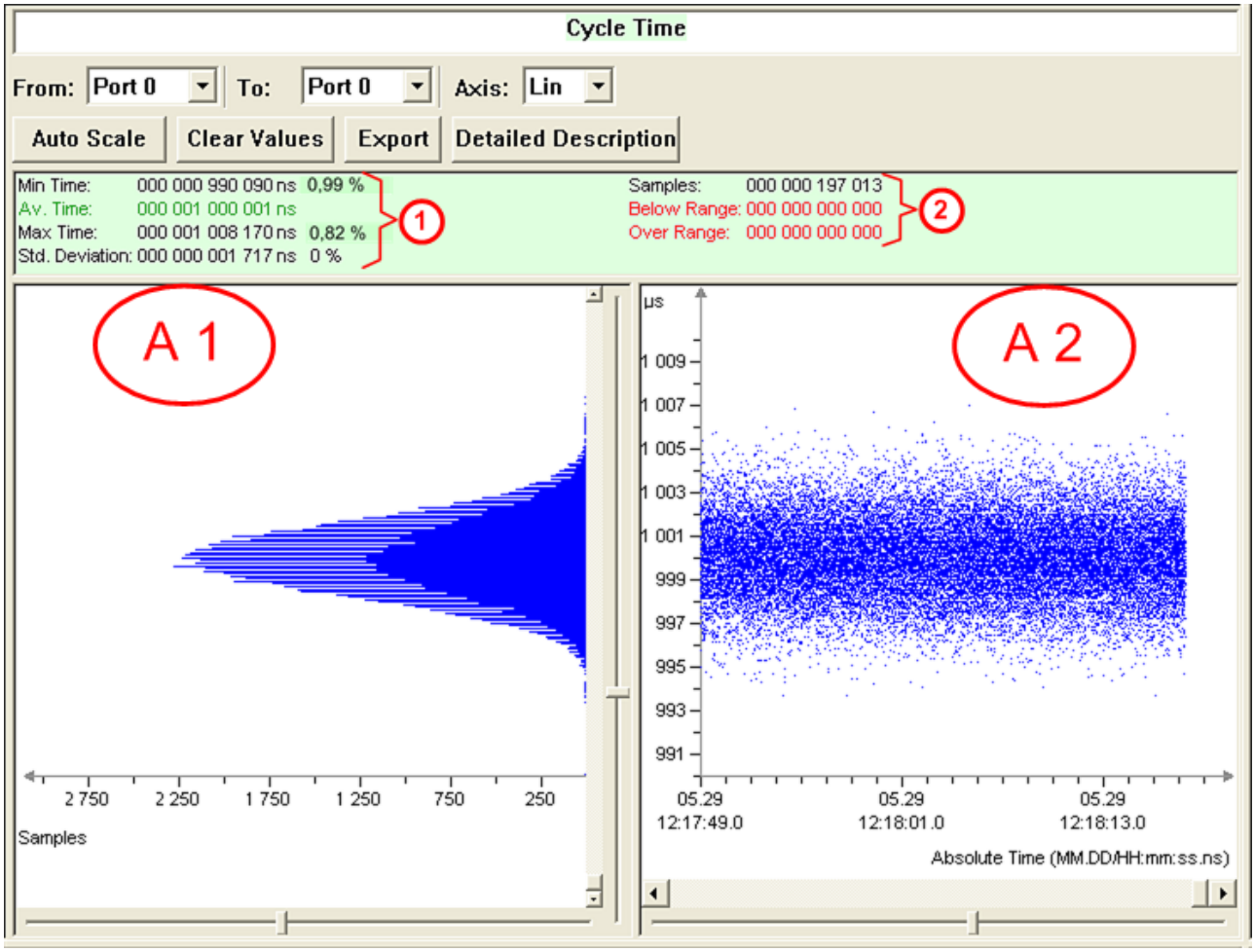


Abbildung 44: EtherCAT Timing-Analysefenster A mit Messdaten

Im Fenster „**A 1**“ (Histogramm) ist die Verteilung der Anzahl der Telegramme über die Zykluszeitabweichung dargestellt.

Im Fenster „**A 2**“ (Historie) ist die Verteilung der Telegramme über die Zeit dargestellt.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Zykluszeit, sowie die prozentuale Abweichung zur mittleren Zykluszeit.	0,99 µs
Av Time	Die mittlere Zykluszeit der Telegramme..	1000,001 µs
Max Time	Die maximale Zykluszeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	1008,170 µs
Std. Deviation	Die Standardabweichung der Zykluszeit.	1,717 µs

© Hilscher, 2008-2012

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	197013
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

Die mittlere Zykluszeit beträgt somit 1 ms. Alle weiteren Messungen, die in der Größenordnung der Zykluszeit liegen, sind Messungen zwischen Hin- und Rückweg des Telegramms. Dies sind in der Regel keine sinnvollen Messungen.

5.2.4.2 Messergebnis Fenster B: Ringdurchlaufzeit

➭ Im Fenster B des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

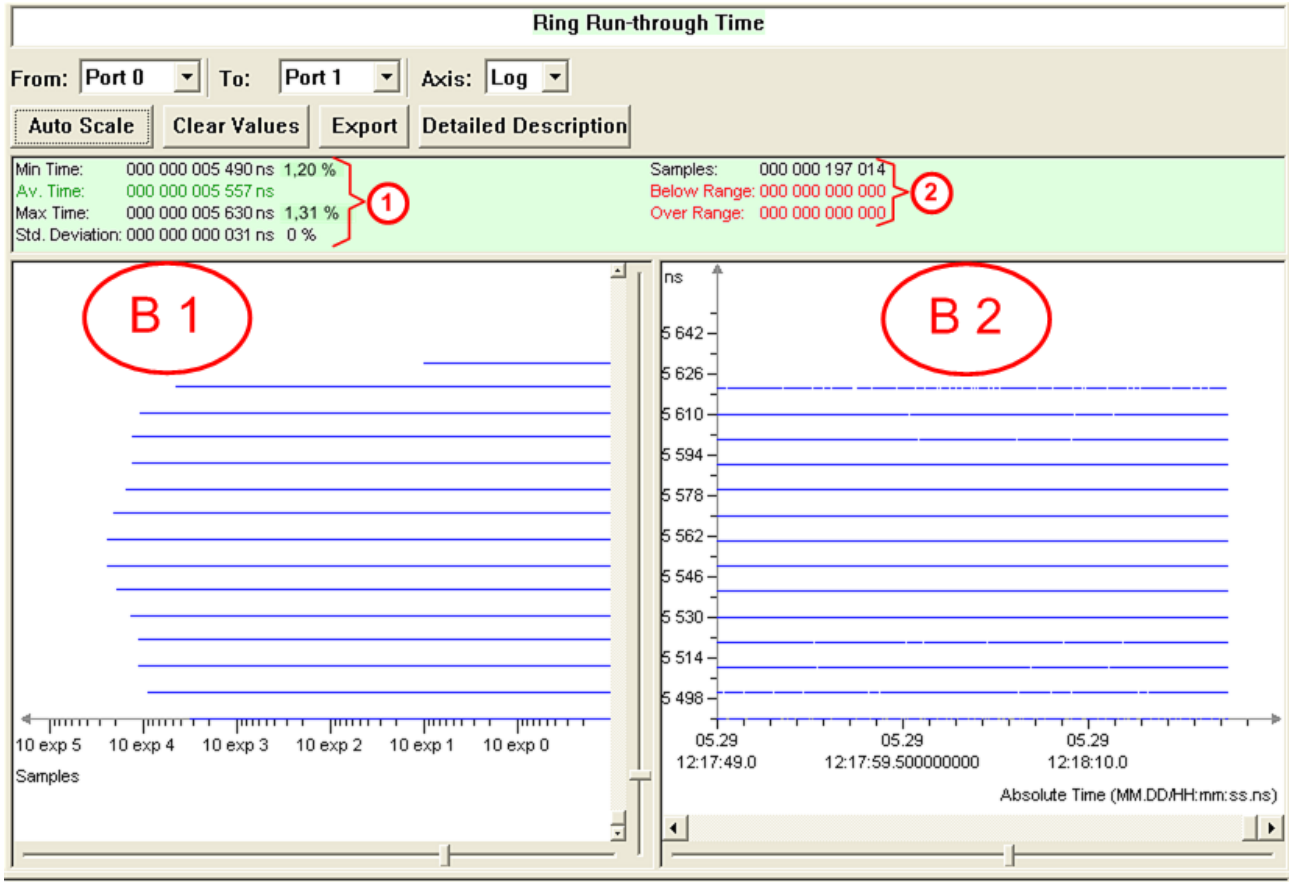


Abbildung 45: EtherCAT Timing-Analysefenster B mit Messdaten

Im Fenster „**B 1**“ (Histogramm) ist die Verteilung der Anzahl der Telegramme über die Ringdurchlaufzeit dargestellt.

Im Fenster „**B 2**“ (Historie) ist die Verteilung der Telegramme über die Zeit dargestellt.

© Hilscher, 2008-2012

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Ringdurchlaufzeit, sowie die prozentuale Abweichung zur mittleren Ringdurchlaufzeit.	5,49 µs
Av Time	Die mittlere Ringdurchlaufzeit der Telegramme..	5,557 µs
Max Time	Die maximale Ringdurchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Ringdurchlaufzeit.	5,63 µs
Std. Deviation	Die Standardabweichung der Ringdurchlaufzeit.	31 ns

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	197014
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

Hier ist zu erkennen, dass die mittlere Ringdurchlaufzeit ca. 5,56 µs beträgt.

Hinweis: Durch die Autocrossover-Funktion der Ethernet-PHYs der EtherCAT-Geräte können bei erneutem Start der Anlage die Ports 0 und 1 gegeneinander vertauscht sein.

© Hilscher, 2008-2012

5.2.4.3 Messergebnis Fenster C: Zykluszeit - Ringdurchlaufzeit

➭ Im Fenster C des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

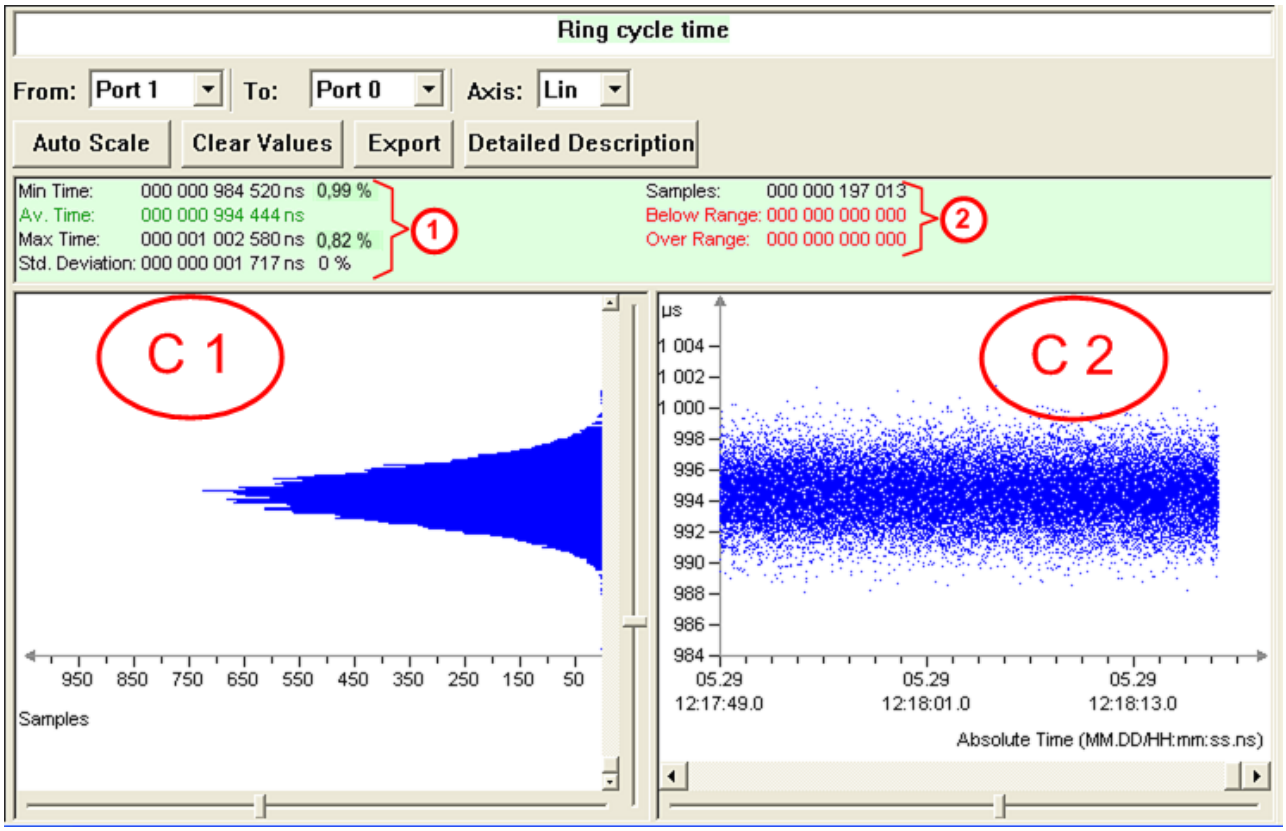


Abbildung 46: EtherCAT Timing-Analysefenster C mit Messdaten

Hier ist zu erkennen, dass dies keine sinnvolle Messung ist, da die ermittelte Protokollfolgezeit im Bereich der Zykluszeit liegt.

Aus dem Messergebnis im Fenster B und Fenster C ist zu erkennen, dass in diesem Aufbau die Signale vom Master über den Port 0 in die netANALYZER-Karte laufen.

© Hilscher, 2008-2012

5.2.4.4 Messergebnis Fenster D: Telegrammdurchlaufzeit durch Slave 1

Im Fenster D des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

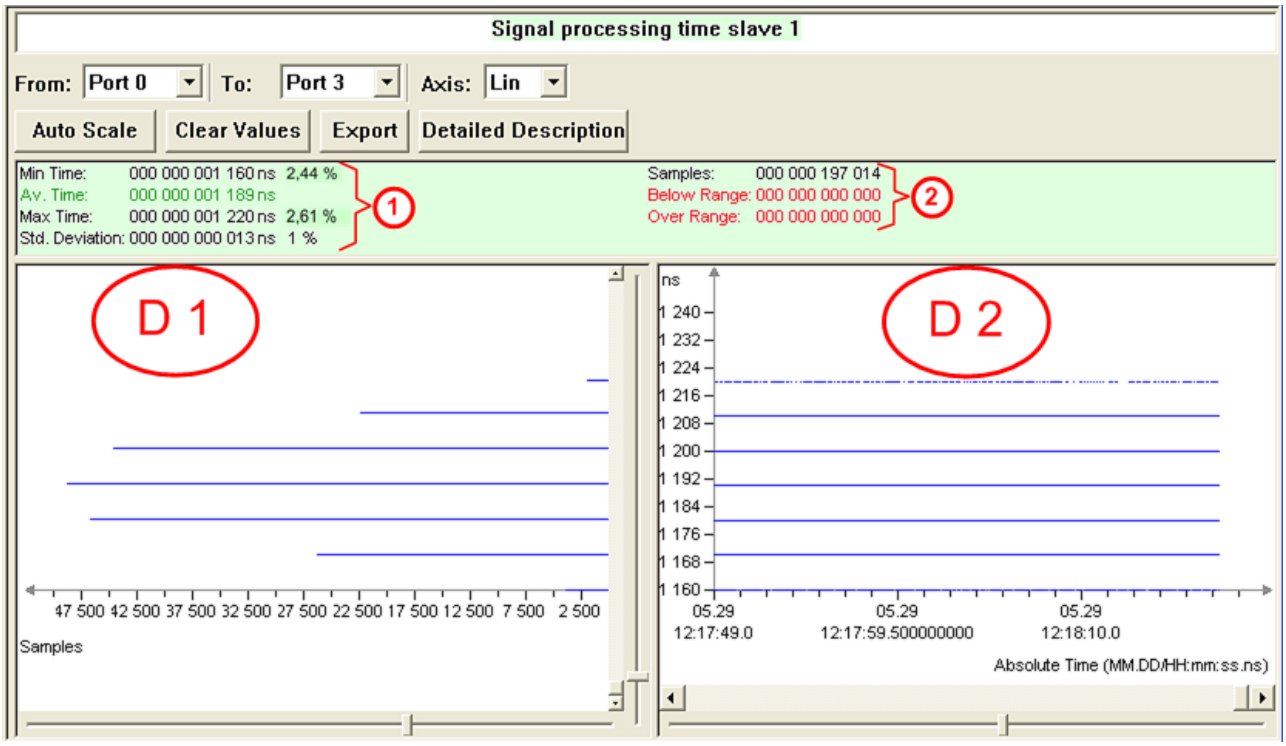


Abbildung 47: EtherCAT Timing-Analysefenster D mit Messdaten

Hier ist zu erkennen, dass die Telegrammdurchlaufzeit durch den Slave 1 gemessen wurde.

Die Einzelstreifen kommen durch die Auflösung der netANALYZER-Karte von 10 ns zustande.

Im Fenster „**D 1**“ (Histogramm) ist die Verteilung der Anzahl der Telegramme über die Ringdurchlaufzeit dargestellt.

Im Fenster „**D 2**“ (Historie) ist die Verteilung der Telegramme über die Zeit dargestellt.

Bei (1) sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Telegrammdurchlaufzeit, sowie die prozentuale Abweichung zur mittleren Zykluszeit.	1,16 µs
Av Time	Die mittlere Telegrammdurchlaufzeit der Telegramme..	1,189 µs
Max Time	Die maximale Telegrammdurchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	1,22 µs
Std. Deviation	Die Standardabweichung der Telegrammdurchlaufzeit.	13 ns

Bei (2) sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	197014
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

5.3 Datenaufzeichnungen durchführen

Es sollen die Telegramme der PC-Karte cifX zu den Slaves und die Antworttelegramme von den Slaves an die PC-Karte cifX aufgezeichnet werden.

Voraussetzungen:

- Der Hardware-Aufbau, wie in *Hardware-Aufbau* auf Seite 42 beschrieben, muss erstellt sein,
- die Einstellungen für die PC-Karte cifX müssen erfolgt sein,
- es muss ein Datenaustausch zwischen der PC-Karte cifX und den Slaves erfolgen,
- es müssen die Grundeinstellungen für den netANALYZER, wie in *Zeitmessung vorbereiten* auf Seite 17 beschrieben, erfolgt sein.

➢ Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

⇘ Sie gelangen ins Hauptfenster des netANALYZERs.

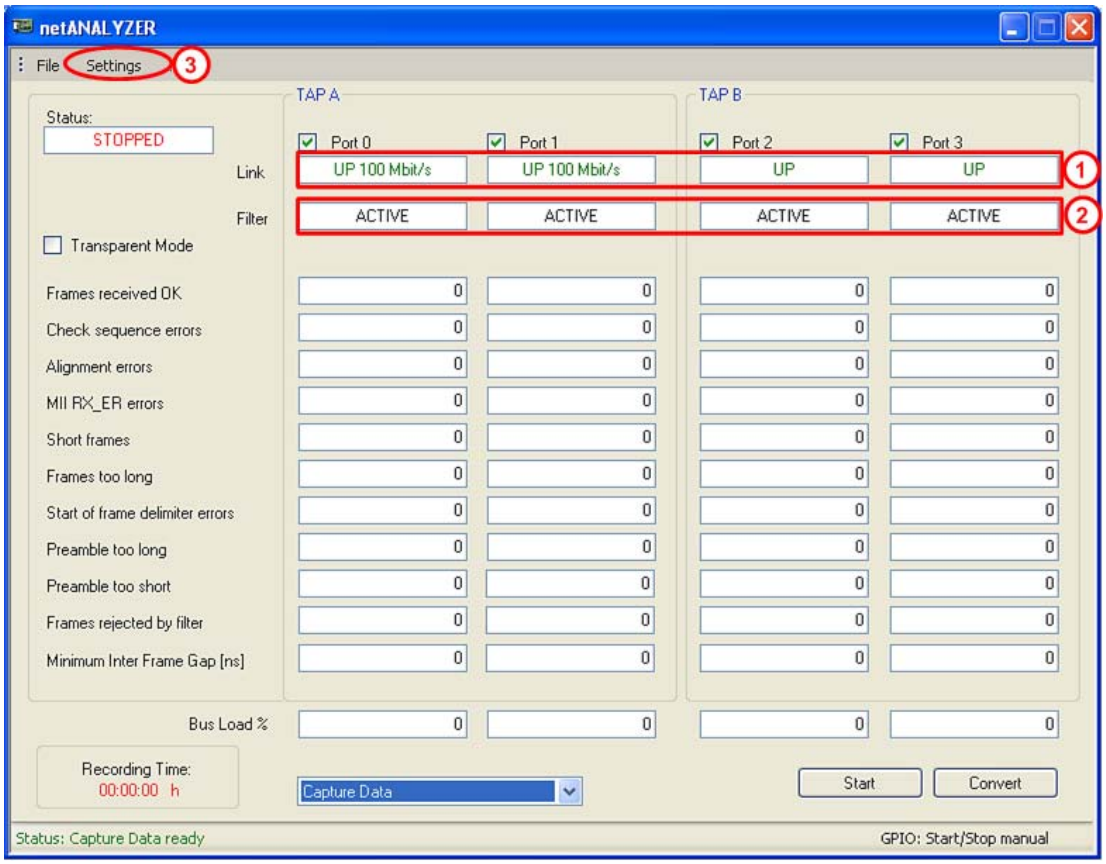


Abbildung 48: EtherCAT netANALYZER Hauptfenster

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 42 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP** gekennzeichnet.

© Hilscher, 2008-2012

- ➢ Stellen Sie sicher, dass der Filter entsprechend Abschnitt *Zeitmessung vorbereiten* Seite 43 eingestellt ist.
- ➢ Verlassen Sie die Filtereinstellungen mit **OK**.
- ➢ Sie kommen zurück ins Hauptfenster.

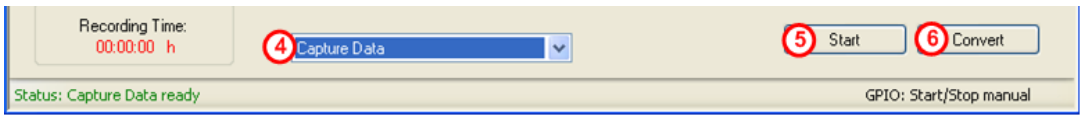


Abbildung 49: Datenaufzeichnung starten

- ➢ Stellen Sie sicher, dass **Capture Data** (4) eingestellt ist.
- ➢ Klicken Sie **Start** (5), um die Aufzeichnung zu starten.
- ➢ Die Schaltfläche **Start** (5) wird zur Schaltfläche **Stop** (5).
- ➢ Warten Sie bis eine ausreichende Anzahl von Telegrammen aufgezeichnet wurden.
- ➢ Klicken Sie **Stop** (5).
- ➢ Klicken Sie **Convert** (6).
- ➢ Es erscheint folgendes Fenster:

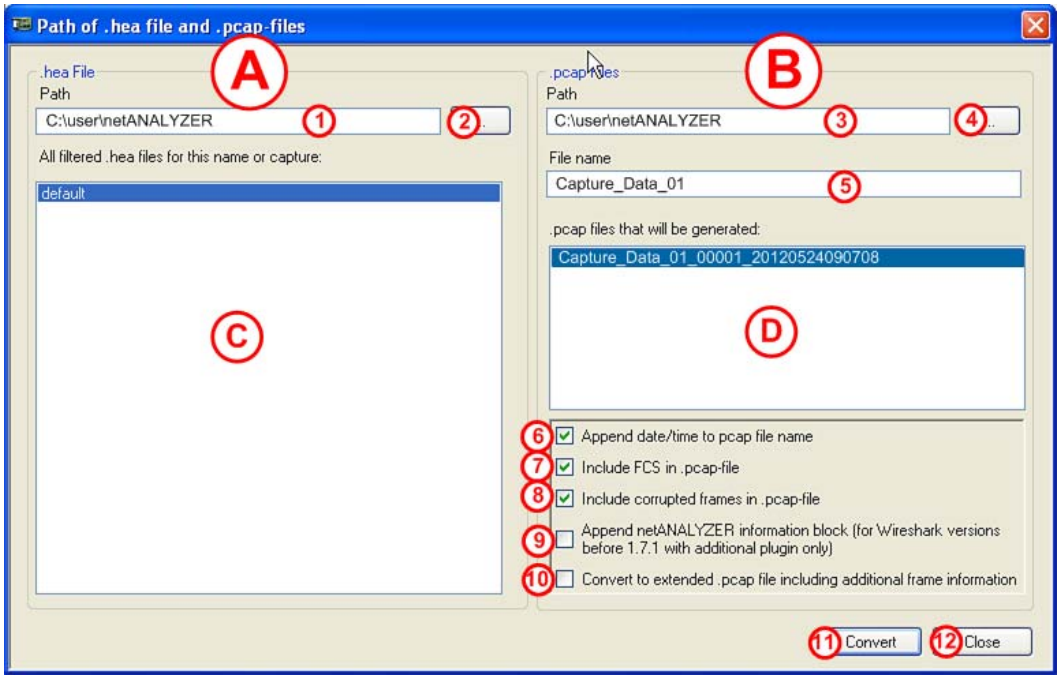


Abbildung 50: pcap-Konvertierung 1

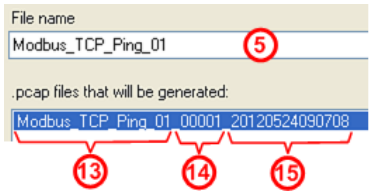
Das obige Fenster teilt sich in zwei Bereiche:

Fensterbereich (A)

Bedienelement	Erläuterung
Path (1)	Vom Bediener auszuwählender Pfad, aus welchem der netANALYZER die Binär-Datei (**.hea*) zur Konvertierung lesen soll. Die hier gemachten Einstellungen wirken sich auch auf die nächsten Datenaufzeichnungen aus. Die Einstellung unter **Settings > File Settings** wird damit verändert.
Schaltfläche (2)	Auswahlschaltfläche zur Auswahl des Quellverzeichnisses der .hea-Dateien.
All filtered .hea files for this name or capture (C)	Anzeigeliste der .hea-Dateien im ausgewähltem Verzeichnis

© Hilscher, 2008-2012

Fensterbereich B

Bedienelement	Erläuterung
Path 3	Der vom Bediener zu definierende Pfad, unter welchem die **netANALYZER**-Software die konvertierte WinPcap-Datei (**.pcap*) ablegen soll.
Schaltfläche 4	Auswahlschaltfläche zur Auswahl des Zielverzeichnis der .pcap-Dateien.
File name 5	Systematische Dateibezeichnung für die **.pcap*-Dateien. Die **netANALYZER**-Software vergibt zusätzlich für jede Datei noch eine fortlaufende Nummer im Dateinamen.
.pcap files that will be generated D	Vorschau der zu erzeugenden **.pcap*-Dateien. Dabei ist der Namensaufbau wie folgt:  13 der unter 5 ausgewählte Dateiname. 14 laufende Zählnummer 15 Zeitinformation, bestehend aus: yyyymmddhhmmss (Beginn der Aufzeichnung der hea-Datei, (nur wenn 6 der Haken gesetzt wurde.).
Append date/time to pcap file name 6	Ist der Haken gesetzt, werden Datum und Zeit im Dateinamen ergänzt.
Include FCS in .pcap-files 7	Checkbox ob die Ethernet-Prüfsumme mit in der PCAP-Datei enthalten sein soll oder nicht. (Einige Wireshark-Dissectoren unterstützen FCS nicht.) **Hinweis:** Wenn **Convert to extended .pcap file including additional frame information** angehakt ist, ist **Include FCS in .pcap-file** ausgegraut, da FCS dann immer in eine .pcap-Datei konvertiert wird. FCS = Frame Check Sequence (Ethernet-Prüfsumme) Nicht auswählbar, wenn Option 10 angehakt, jedoch aktiv.
Include corrupted frames in .pcap file 8	Ist diese Option aktiviert, werden auch fehlerhafte Frames in die .pcap-Datei übernommen. Ist die Option deaktiviert werden nur korrekte Telegramme in der .pcap-Datei gespeichert.
Append netANALYZER information block (for Wireshark versions before 1.7.1 with additional plug in only) 9	Die Option erfordert für Wireshark-Versionen < V1.7.1 die Installation des netANALYZER-Wireshark-Plugins. Fügt den netANALYZER-Info-Block nach dem Ethernet-Frame in die .pcap-Dateien ein. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen. **Hinweis:** Das .pcap-Dateiformat mit dem Info-Block nach dem Ethernet-Frame wird von Wireshark-Versionen ≥ 1.7.1 nicht mehr unterstützt. Nicht auswählbar, wenn Option 10 angehakt.
Convert to extended .pcap file including additional frame information 10	**Hinweis:** Wird dieser Haken gesetzt, kann das mit der netANALYZER-Software V1.4.x.x erzeugte erweiterte .pcap-Dateiformat nur in Wireshark-Versionen ab V1.7.1 geöffnet werden. Ab der Version der netANALYZER-Software V1.4.x.x kann ein erweitertes .pcap-Dateiformat erzeugt werden. Dabei befindet sich der „netANALYZER Info-Block“ in den 4 Bytes vor dem Ethernet-Frame. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen.
Convert 11	Die Konvertierung der Binär-Dateien ins WinPcap-Format wird gestartet.
Close 12	Sie schließen das Fenster ohne eine Konvertierung zu starten.

- ➢ Wählen Sie im Fensterbereich A die zu konvertierende Datei aus.
- ➢ Ergänzen Sie die notwendigen Einstellungen im Fensterbereich B.
- ➢ Klicken Sie auf die Schaltfläche **Convert** 11, um die Daten ins pcap-Format zu konvertieren.
- ➢ Nach Abschluss des Konvertierungsvorgangs schließt sich das Fenster.

© Hilscher, 2008-2012

➢ Öffnen Sie die Datei mit Wireshark.
Wenn das Programm Wireshark korrekt installiert ist, wird mittels eines Doppelklicks auf die .pcap-Datei diese mit Wireshark geöffnet.

↬ Es werden folgende Daten angezeigt:

➢ Doppelklick auf die konvertierte Datei (hier c:\Default_001.pcap), oder starten Sie das Programm Wireshark und gehen Sie über den Menüpfad **File > Open** und wählen die Datei aus.

↬ Das Programm Wireshark zeigt die Daten wie folgt an:

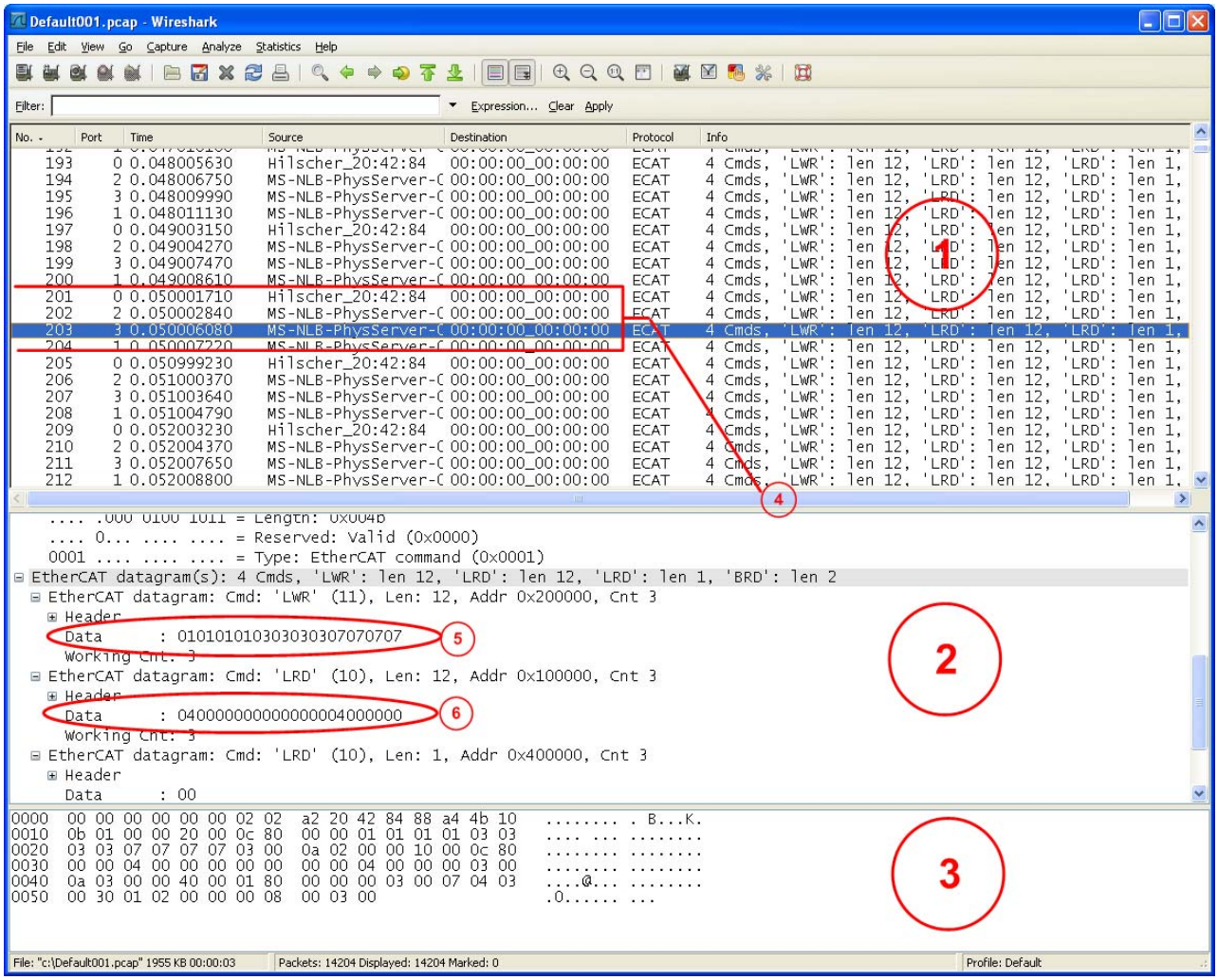

Default001.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Port Time Source Destination Protocol Info
193 0 0.048005630 Hilscher_20:42:84 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
194 2 0.048006750 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
195 3 0.048009990 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
196 1 0.048011130 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
197 0 0.049003150 Hilscher_20:42:84 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
198 2 0.049004270 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
199 3 0.049007470 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
200 1 0.049008610 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
201 0 0.050001710 Hilscher_20:42:84 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
202 2 0.050002840 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
203 3 0.050006080 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
204 1 0.050007220 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
205 0 0.050999230 Hilscher_20:42:84 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
206 2 0.051000370 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
207 3 0.051003640 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
208 1 0.051004790 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
209 0 0.052003230 Hilscher_20:42:84 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
210 2 0.052004370 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
211 3 0.052007650 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
212 1 0.052008800 MS-NLB-PhysServer-C 00:00:00_00:00:00 ECAT 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1,
1
4
.... .000 0100 1011 = Length: 0x004B
.... 0... .... = Reserved: Valid (0x0000)
0001 .... = Type: EtherCAT command (0x0001)
EtherCAT datagram(s): 4 Cmds, 'LWR': len 12, 'LRD': len 12, 'LRD': len 1, 'BRD': len 2
EtherCAT datagram: Cmd: 'LWR' (11), Len: 12, Addr 0x200000, Cnt 3
Header
Data : 0101010103030307070707
5
Working Cnt: 3
EtherCAT datagram: Cmd: 'LRD' (10), Len: 12, Addr 0x100000, Cnt 3
Header
Data : 040000000000000004000000
6
Working Cnt: 3
EtherCAT datagram: Cmd: 'LRD' (10), Len: 1, Addr 0x400000, Cnt 3
Header
Data : 00
2
0000 00 00 00 00 00 00 02 02 a2 20 42 84 88 a4 4b 10 ..... . B...K.
0010 0b 01 00 00 20 00 0c 80 00 00 01 01 01 01 03 03 ....
0020 03 03 07 07 07 07 03 00 0a 02 00 00 10 00 0c 80 ....
0030 00 00 04 00 00 00 00 00 00 00 04 00 00 00 03 00 ....
0040 0a 03 00 00 40 00 01 80 00 00 00 03 00 07 04 03 ....@... .....
0050 00 30 01 02 00 00 00 08 00 03 00 .0..... ...
3
File: "c:\Default001.pcap" 1955 KB 00:00:03
Packets: 14204 Displayed: 14204 Marked: 0
Profile: Default

Abbildung 51: EtherCAT Wireshark Daten

① In diesem Fensterbereich sehen Sie die Auflistung aller Telegramme.

② In diesem Fensterbereich können Sie einzelne Telegrammbereiche des ausgewählten Telegramms betrachten.

③ In diesem Fensterbereich werden die Daten des ausgewählten Telegramms auf Byteebene dargestellt.

④ Hier ist ein kompletter Telegrammzyklus des Messaufbaus gekennzeichnet. Die erste Zeile enthält das Telegramm wie es vom Master kommt. Dieses wurde am Port 0 aufgezeichnet.

Die zweite Zeile enthält das Telegramm nach dem ersten Slave auf dem Weg zum Slave 2 und 3. Dieses wurde am Port 2 aufgezeichnet.

Die dritte Zeile enthält das Telegramm, wie es vom Slave 2 zurück kommt, nachdem es bereits im Slave 3 bearbeitet wurde. Dieses wurde am Port 3 aufgezeichnet.

© Hilscher, 2008-2012

Die vierte Zeile enthält das Telegramm, wie es vom Slave 1 an den Master zurückgesendet wird. Dieses wurde am Port 1 aufgezeichnet.

⑤ Hier ist der Teil des Telegramms (dritte Zeile des Zyklus) gekennzeichnet, der die Sollwerte an die Slaves beinhaltet.

⑥ Hier ist der Teil des Telegramms (dritte Zeile des Zyklus) gekennzeichnet, der die Istwerte aus den Slaves beinhaltet.

© Hilscher, 2008-2012

6 EtherNet/IP Analyse

Beispielhaft werden hier folgende Messungen durchgeführt:

- Messung der Zykluszeit zu Slave 3,
- Messung der Zykluszeit vom Slave 3,
- Messung der Durchlaufzeit durch Slave 1 und 2 in beiden Signalrichtungen,
- Messung der Netzlast mit EtherNet/IP-Telegrammen beim Netzwerkanlauf und Ping.

6.1 Hardware-Aufbau

Für diese Beispielmessung wird folgender Hardware-Aufbau benötigt.

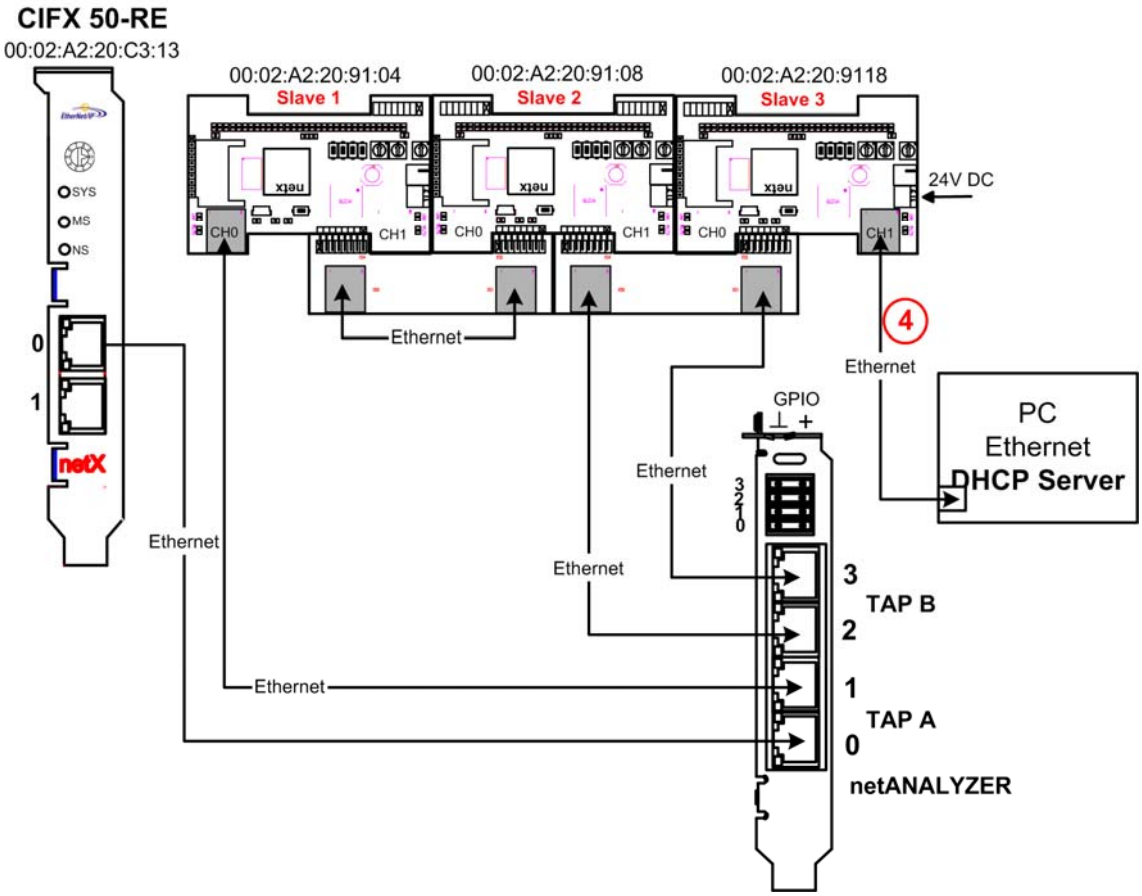


Abbildung 52: EtherNet/IP Hardware-Aufbau

Die für den in diesem Aufbau geltenden MAC-Adressen sind oberhalb der Komponenten angegeben.

Beachten Sie bitte, dass die jeweilige MAC-Adresse auf der Welt einmalig ist. Daher haben die Geräte in Ihrem Messaufbau andere MAC-Adressen.

Hinweis: Die Einstellungen für die PC-Karte cifX und die NXIO 50 Boards müssen entsprechend Abschnitt 6.4 des *Benutzerhandbuch Real-Time-Ethernet-Kit - Kommunikationssysteme für Real-Time-Ethernet Installation, Bedienung und Konfiguration* vorgenommen worden sein.

© Hilscher, 2008-2012

6.2 Datenaufzeichnung durchführen

Es ist die Verbindungs-ID des Slave 3 für die zyklische Datenübermittlung des Slaves zu ermitteln.

Diese Information benötigen Sie für die Filtereinstellungen, wenn Sie mit der Timing Analyse Laufzeiten von Slave-Telegrammen ermitteln wollen.

- Es sind sämtliche Filter auszuschalten, damit alle Telegramme erfasst werden können.

Gehen Sie dazu wie folgt vor:

- Stoppen Sie jegliche Datenerfassung.
- Im Hauptfenster des netANALYZERs wählen Sie **Settings** > **Filters Settings** aus.

Es öffnet sich das Fenster der Filtereinstellungen.

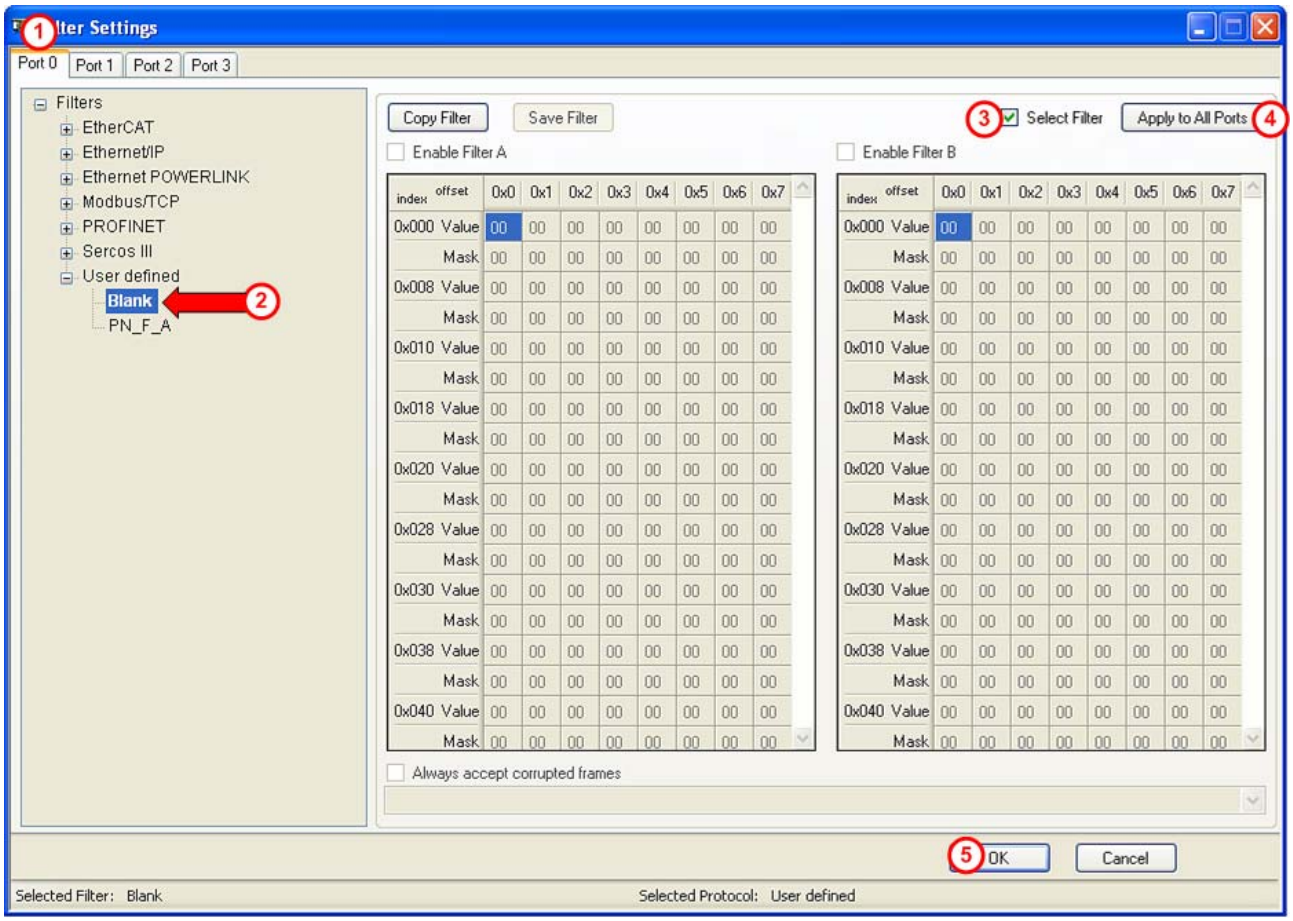


Abbildung 53: EtherNet/IP Filter Data Capture

- Wählen Sie **Port 0** (1).
- Wählen Sie unter **User Defined** Blank (2) aus.
- Haken Sie **Select Filter** (3) an.
- Weisen Sie diese Einstellungen allen Ports mit Klick auf **Apply to All Ports** (4) zu.
- Schließen Sie das Fenster mit **OK** (5).

© Hilscher, 2008-2012

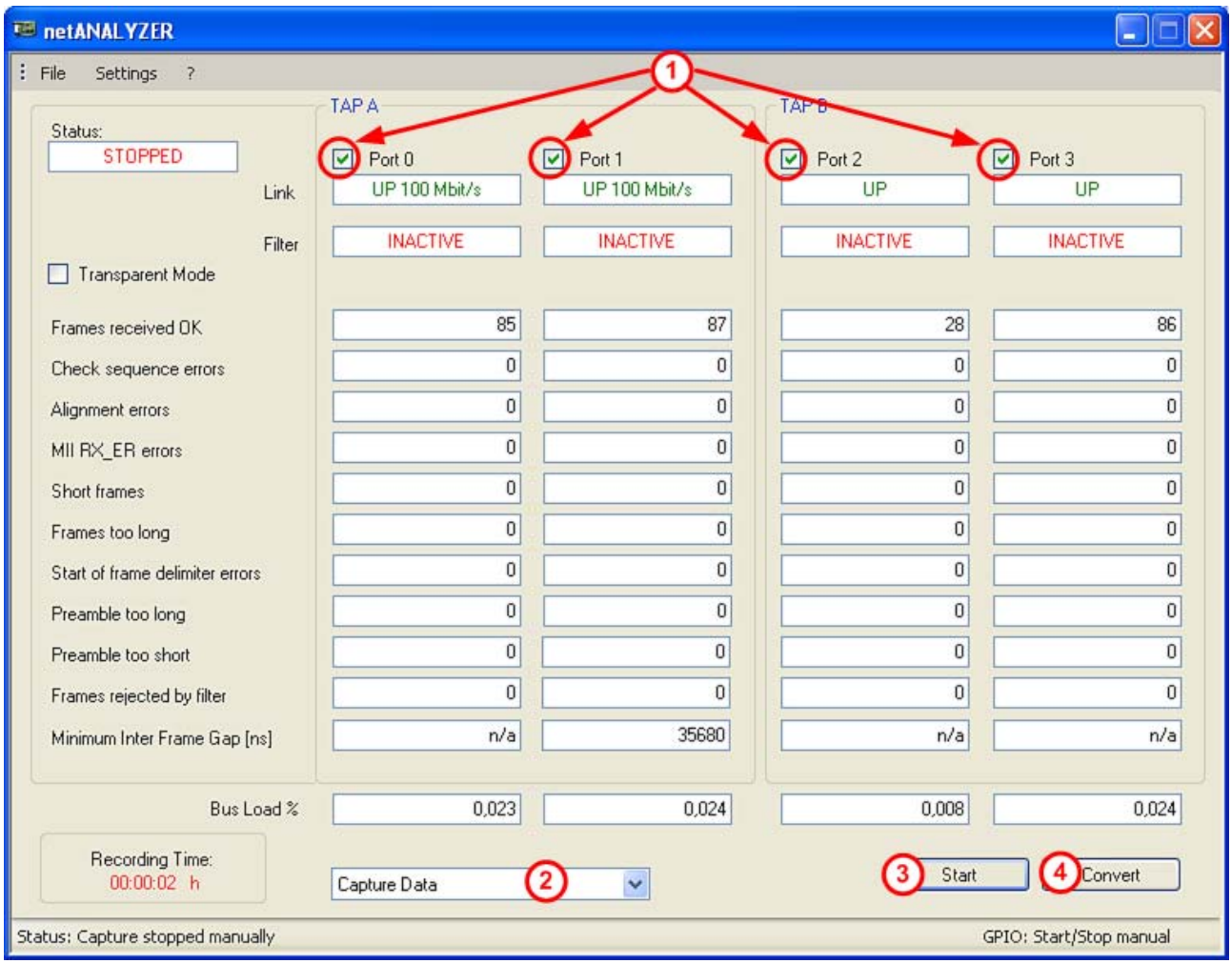


Abbildung 54: EtherNet/IP Data Capture Start

- Achten Sie darauf, dass alle Ports für die Datenaufzeichnung ausgewählt sind (1).
- Wählen Sie **Capture Data** (2) aus.
- Starten Sie die Aufzeichnung mit **Start** (3).
- Die Datenaufzeichnung beginnt, die Start-Schaltfläche wurde zur Stop-Schaltfläche.
- Warten Sie, bis einige Telegramme erfasst wurden.
- Klicken Sie **Stop** (3) und anschließend **Convert,** um die Daten ins pcap-Format, zur Analyse im Wireshark zu konvertieren.

© Hilscher, 2008-2012

Es öffnet sich folgendes Fenster:

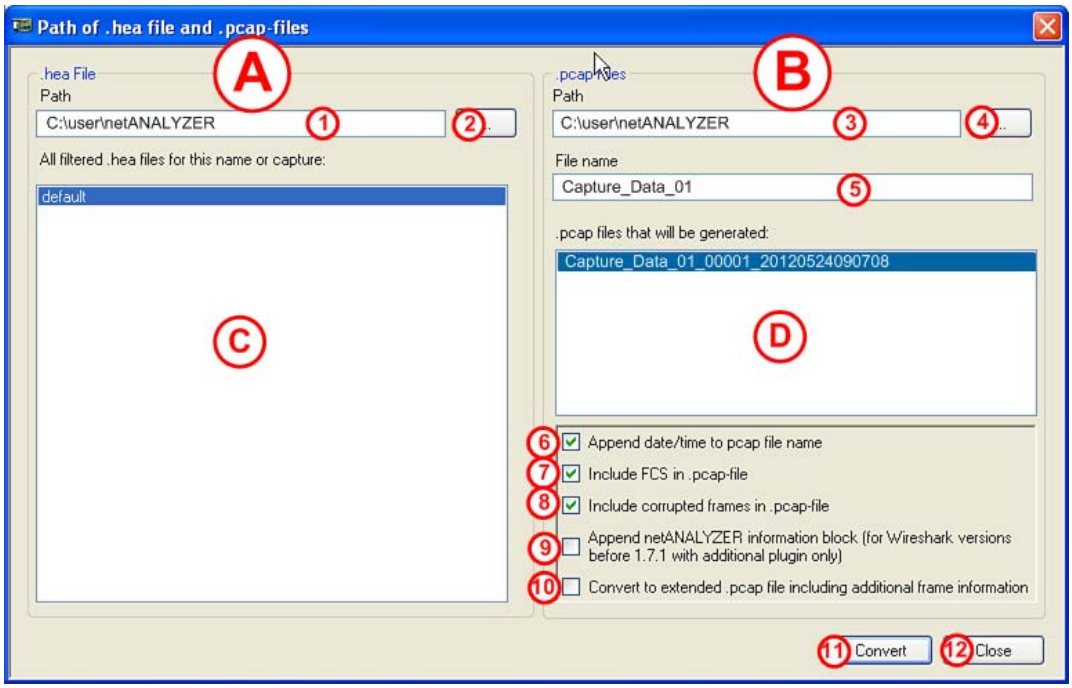


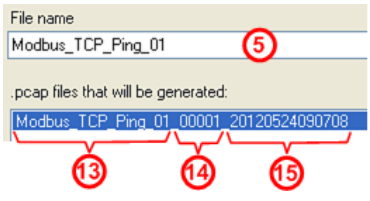
Abbildung 55: Ethernet/IP netANALYZER Analyse Convertierung 1

Das obige Fenster teilt sich in zwei Bereiche:

Fensterbereich Ⓐ

Bedienelement	Erläuterung
Path ①	Vom Bediener zu definierender Pfad, aus welchem der netANALYZER die Binär-Datei (**.hea*) zur Konvertierung lesen soll. Die hier gemachten Einstellungen wirken sich auch auf die nächsten Datenaufzeichnungen aus. Die Einstellung unter **Settings > File Settings** wird damit verändert.
Schaltfläche ②	Auswahlschaltfläche zur Auswahl des Quellverzeichnisses der .hea-Dateien.
All filtered .hea files for this name or capture Ⓒ	Anzeigeliste der .hea-Dateien im ausgewähltem Verzeichnis

Fensterbereich Ⓑ

Bedienelement	Erläuterung
Path ③	Der vom Bediener zu definierende Pfad, unter welchem die **netANALYZER**-Software die konvertierte WinPcap-Datei (**.pcap*) ablegen soll.
Schaltfläche ④	Auswahlschaltfläche zur Auswahl des Zielverzeichnis der .pcap-Dateien.
File name ⑤	Systematische Dateibezeichnung für die **.pcap*-Dateien. Die **netANALYZER**-Software vergibt zusätzlich für jede Datei noch eine fortlaufende Nummer im Dateinamen.
.pcap files that will be generated Ⓓ	Vorschau der zu erzeugenden **.pcap*-Dateien. Dabei ist der Namensaufbau wie folgt:  ⑬ der unter ⑤ ausgewählte Dateiname. ⑭ laufende Zählnummer ⑮ Zeitinformation, bestehend aus: yyyymmddhhmmss (Beginn der Aufzeichnung der hea-Datei, (nur wenn ⑥ der Haken gesetzt wurde.).
Append date/time to pcap file name ⑥	Ist der Haken gesetzt, werden Datum und Zeit im Dateinamen ergänzt.

© Hilscher, 2008-2012

Bedienelement	Erläuterung
Include FCS in .pcap-files (7)	Checkbox ob die Ethernet-Prüfsumme mit in der PCAP-Datei enthalten sein soll oder nicht. (Einige Wireshark-Dissectoren unterstützen FCS nicht.) **Hinweis:** Wenn **Convert to extended .pcap file including additional frame information** angehakt ist, ist **Include FCS in .pcap-file** ausgegraut, da FCS dann immer in eine .pcap-Datei konvertiert wird. FCS = Frame Check Sequence (Ethernet-Prüfsumme) Nicht auswählbar, wenn Option (10) angehakt, jedoch aktiv.
Include corrupted frames in .pcap file (8)	Ist diese Option aktiviert, werden auch fehlerhafte Frames in die .pcap-Datei übernommen. Ist die Option deaktiviert werden nur korrekte Telegramme in der .pcap-Datei gespeichert.
Append netANALYZER information block (for Wireshark versions before 1.7.1 with additional plug in only) (9)	Die Option erfordert für Wireshark-Versionen < V1.7.1 die Installation des netANALYZER-Wireshark-Plugins. Fügt den netANALYZER-Info-Block nach dem Ethernet-Frame in die .pcap-Dateien ein. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen. **Hinweis:** Das .pcap-Dateiformat mit dem Info-Block nach dem Ethernet-Frame wird von Wireshark-Versionen ≥ 1.7.1 nicht mehr unterstützt. Nicht auswählbar, wenn Option (10) angehakt.
Convert to extended .pcap file including additional frame information (10)	**Hinweis:** Wird dieser Haken gesetzt, kann das mit der netANALYZER-Software V1.4.x.x erzeugte erweiterte .pcap-Dateiformat nur in Wireshark-Versionen ab V1.7.1 geöffnet werden. Ab der Version der netANALYZER-Software V1.4.x.x kann ein erweitertes .pcap-Dateiformat erzeugt werden. Dabei befindet sich der „netANALYZER Info-Block“ in den 4 Bytes vor dem Ethernet-Frame. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen.
Convert (11)	Die Konvertierung der Binär-Dateien ins WinPcap-Format wird gestartet.
Close (12)	Sie schließen das Fenster ohne eine Konvertierung zu starten.

- ➢ Wählen Sie im Fensterbereich (A) die zu konvertierende Datei aus.
- ➢ Ergänzen Sie die notwendigen Einstellungen im Fensterbereich (B).
- ➢ Klicken Sie **Convert** (11), um die Daten ins pcap-Format zu konvertieren.
- ↬ Nach Abschluss des Konvertierungsvorgangs schließt sich das Fenster.
- ➢ Öffnen Sie die Datei mit Wireshark.
  Wenn das Programm Wireshark korrekt installiert ist, wird mittels eines Doppelklicks auf die .pcap-Datei diese mit Wireshark geöffnet.
- ↬ Es werden folgende Daten angezeigt:

© Hilscher, 2008-2012

6.2.1 Verbindungs-ID ermitteln

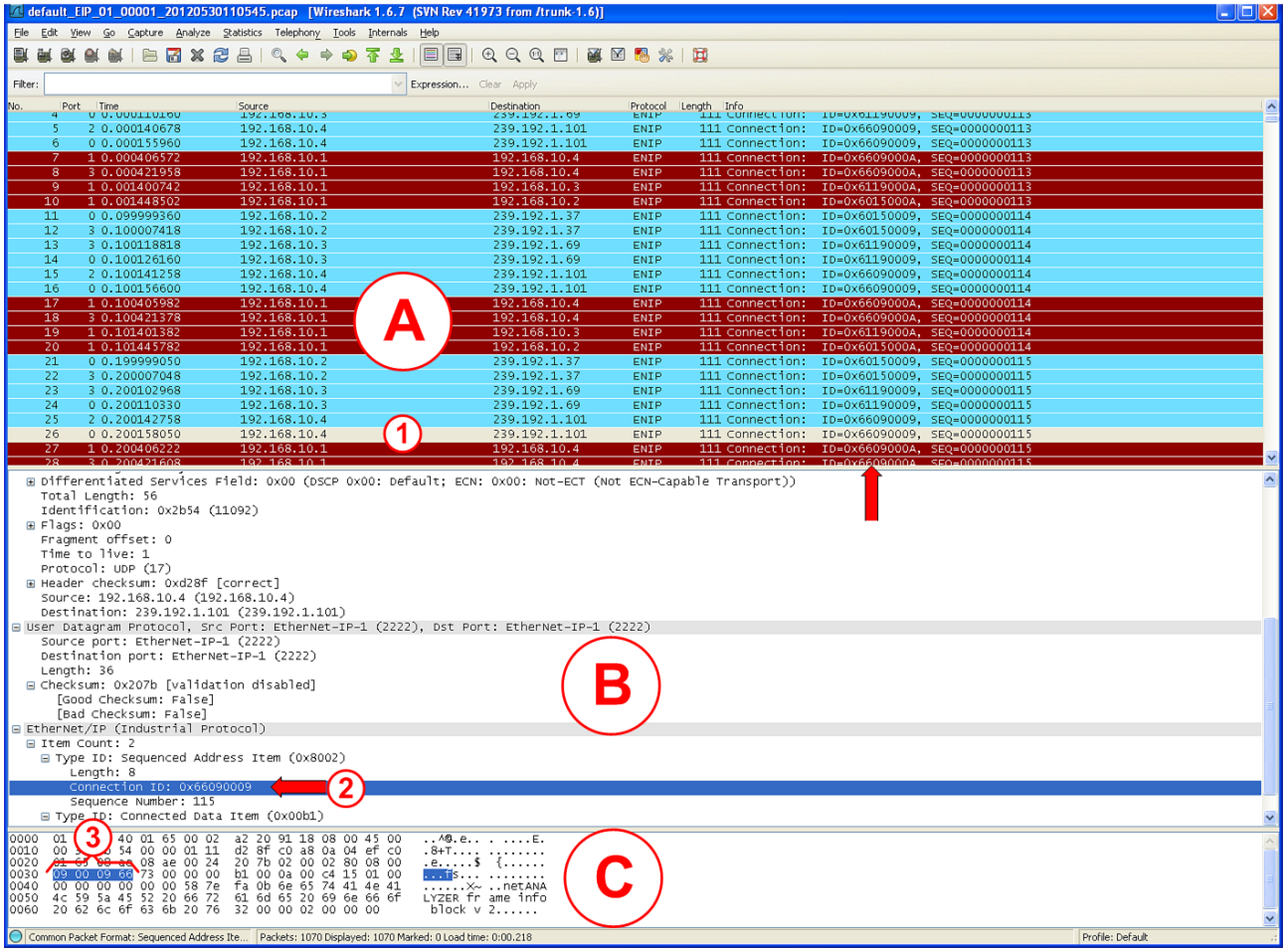


Abbildung 56: EtherNet/IP Data Capture

- Wählen Sie im Fensterbereich Ⓐ ein Telegramm aus, welches vom Slave 3 zyklisch versendet wird.
- Identifizieren Sie im Fensterbereich Ⓑ den Datensatz **Connection ID** und markieren ihn.
- Im Fensterbereich Ⓒ wird Ihnen dieser mit der Datenposition im Telegramm angezeigt ③.

Diese Information benötigen Sie für die Filtereinstellungen, wenn Sie mit der Timing Analyse Laufzeiten von Slave-Telegrammen ermitteln wollen.

Wichtig: Unterbrechen Sie nicht mehr die Datenkommunikation in der Messeinrichtung, da sich mit einem Neustart der Datenkommunikation die „Connection ID“ verändert.

© Hilscher, 2008-2012

6.3 Zeitmessung vorbereiten und durchführen

Hinweis: Die PC-Karte cifX und die NXIO-Boards verfügen über eine Autocrossover-Funktionalität. Daher ist ein Vertauschen der Kabel am netANALYZER am TAP A (Port 0 und Port 1) sowie am TAP B (Port 2 und Port 3) ohne Bedeutung. Somit sind auch bei der Anzeige der Analysewerte die Portbezeichnungen 0/1 bzw. 2/3 als vertauschbar zu betrachten.

Hinweis: Hier sind nur die für diesen Messaufbau unmittelbar erforderlichen Einstellungen des netANALYZERs beschrieben. Detaillierte Informationen über die Einstell- und Aufzeichnungsmöglichkeiten der Software entnehmen Sie bitte der Dokumentation *Benutzerhandbuch netANALYZER NANL-C500-RE*.

Da bei Ethernet/IP der Slave eigenständig im Netzwerk seine Eingangsdaten zyklisch an eine Broadcastadresse sendet, ist es hier notwendig vor der Messung der Slave-Telegramme die Verbindungs-ID für die zyklischen Protokolle des Slaves zu ermitteln.

Diese Verbindungs-ID kann mit einer Datenaufzeichnung ermittelt werden, siehe Abschnitt *Datenaufzeichnung durchführen* Seite 59 bzw. Abschnitt *Verbindungs-ID ermitteln* Seite 63.

Hinweis: Die Verbindungs-ID wird mit jedem Netzwerkanlauf neu ermittelt!

6.3.1 Zeitmessung vorbereiten

Es sollen beispielhaft die Zeiten des Telegrammverlaufs von der PC-Karte cifX (Master) zum NXIO-Board Slave 3 und zurück gemessen werden.

Es ist möglich beide Signalrichtungen in einer gemeinsamen Messung zu erfassen.

- Es ist die MAC-Adresse der PC-Karte cifX zu ermitteln.
  Ist die MAC-Adresse nicht bekannt, können Sie diese wie folgt ermitteln: Verbinden Sie den PC-Ethernet-Netzwerkanschluss mit dem Ethernet-Anschluss der PC-Karte cifX. Starten Sie das Programm „Ethernet Device Configuration“ mit **Start > Programme > SYCON.net Systemkonfigurator > Ethernet-Geräte Setup**
  Klicken Sie **Geräte suchen** im Hauptfenster des Programms. Sie erkennen die PC-Karte cifX an dem Gerätetyp **cifX**.
- Die MAC-Adressen der NXIO Bords ermitteln Sie entsprechend der Beschreibung „Benutzerhandbuch Real-Time-Ethernet-Kit“ in Abschnitt EtherNet/IP.
- Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

© Hilscher, 2008-2012

➭ Sie gelangen ins Hauptfenster des netANALYZERs.

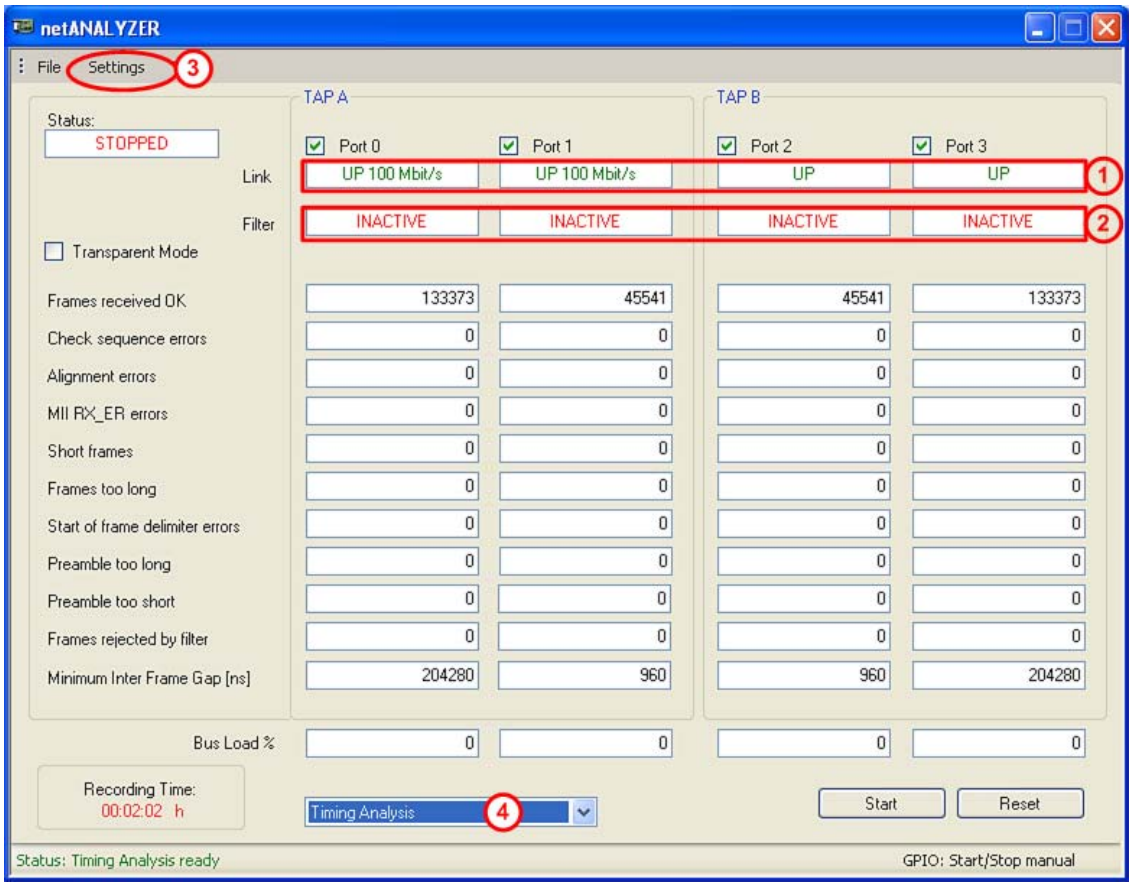


Abbildung 57: EtherNet/IP netANALYZER Hauptfenster

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 58 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP mit Datenrate** oder bei älteren netANALYZER-Karten bei TAP B nur mit **UP** gekennzeichnet.

© Hilscher, 2008-2012

6.3.2 Filter einstellen

➢ Gehen Sie vom Hauptfenster des Programms mit **Settings > Filter Settings** ③ in die Filtereinstellungen.

➢ Es erscheint folgendes Dialogfenster.

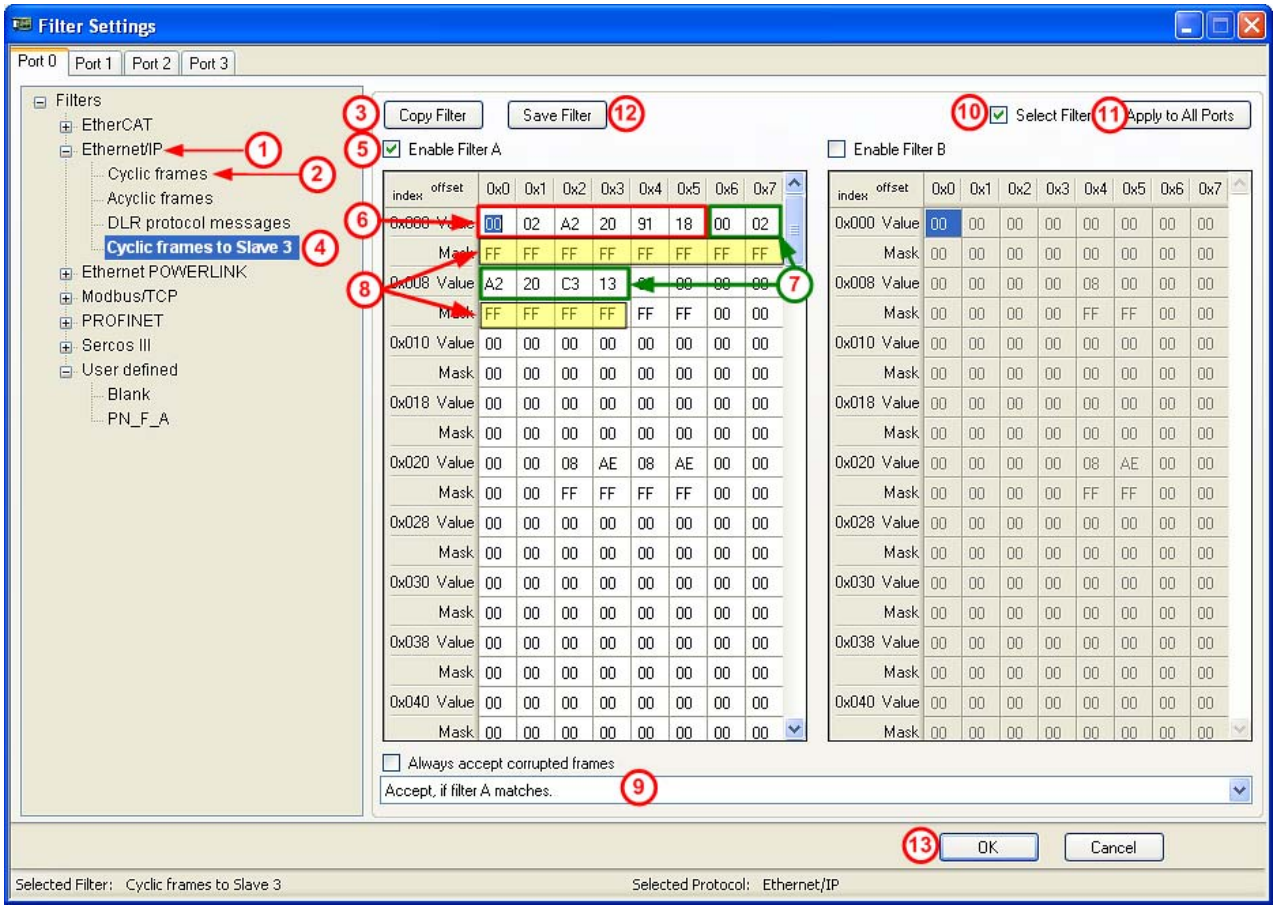


Abbildung 58: EtherNet/IP netANALYZER Filter cifX → Slave 3

Zunächst stellen Sie für alle Ports einen identischen Filter ein. Hier wurde die Kommunikationsrichtung cifX > Slave 3 gewählt.

➢ Wählen Sie **Filters > Ethernet/IP** ① **> Cyclic frames** ②.

➢ Kopieren Sie diesen Filter mit **Copy Filter** ③.

➢ Vergeben Sie einen neuen Namen (hier **Cyclic frames to Slave 3** ④) für den Filter.

➢ Setzen Sie einen Hacken vor **Enable Filter A** ⑤.

Ziel-MAC-Adresse

➢ Geben Sie in den markierten Bereich die MAC-Zieladresse ⑥ (von Slave 3) ein.

Quell MAC-Adresse

➢ Geben Sie in den markierten Bereich die MAC-Adresse ⑦ der PC-Karte cifX ein,

Hinweis: Für Ihren Messaufbau sind die MAC-Adressen entsprechend der von Ihnen verwendeten Geräte anzupassen.

© Hilscher, 2008-2012

Filter Maske

- Tragen Sie in die **Mask** Felder (8) unter der Zeil- und Quelladresse „**FF**“ ein, damit jedes Zeichen in der Ziel- und Quelladresse beim Vergleich berücksichtigt wird.
- Wählen Sie **Accept, if filter A matches** (9) aus,
- Selektieren Sie diesen Filter für Port 0, indem Sie den Haken mit der Maus vor **Select Filter** (10) setzen.
- Klicken Sie **Apply to All Ports** (11), damit diese Filtereinstellung an allen Ports wirksam wird.
- Speichern Sie die Filtereinstellungen mit **Save Filter** (12).

Bei einer Messung werden jetzt an allen Ports der netANALYZER-Karte die zyklischen Telegramme von der PC-Karte cifX zum Slave 3 erfasst. Alle anderen Telegramme werden verworfen.

- Verlassen Sie die Filtereinstellungen mit **OK** (13).

6.3.2.1 Port Signalfluss zuordnen

Hinweis: Durch die Autocrossover-Funktionalität der Geräte können Port 0 und 1 sowie Port 2 und 3 bei Ihrem Versuchsaufbau vertauscht sein!

- Starten Sie einen kurzen Messzeitraum.
- Im Hauptfenster des netANALYZERs bekommen Sie etwa folgende Anzeige.

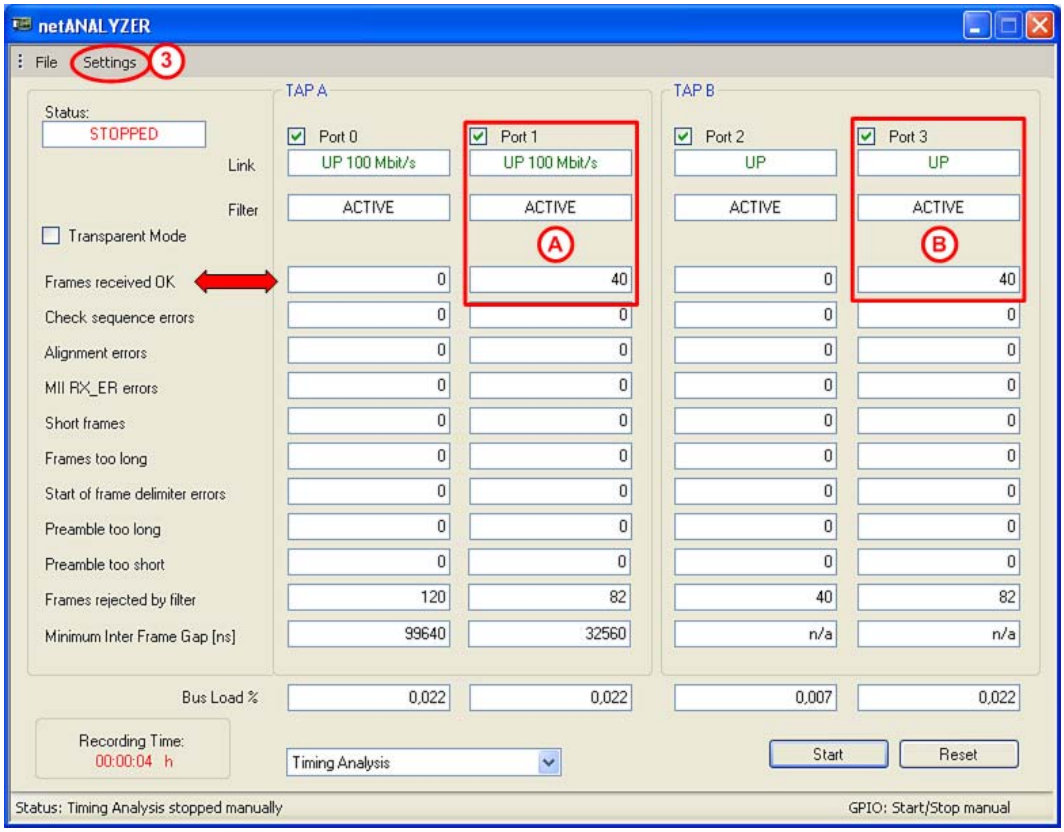


Abbildung 59: EtherNet/IP netANALYZER Signalflussrichtung

Es ist im roten Kasten (A) und (B) in der Zeile **Frames received OK** unter Port 1 und Port 3 zu erkennen, dass an diesen Ports Telegramme von der cifX zum Slave 3 detektiert wurden.

© Hilscher, 2008-2012

Daraus ist zu schließen, dass die Telegramme vom Slave 3 zur PC-Karte cifX über den Port 2 und den Port 0 der netANALYZER-Karte laufen.

Hinweis: Durch die Auto-Cross-Over Funktionalität der Komponenten können bei Ihrem Messaufbau Die Signale auch über den Port 0 und 2 laufen..

Für diese Ports sind jetzt die Filter entsprechend zu setzen.

6.3.2.2 Filter für Signalrichtung vom Slave 3 zur cifX erstellen

Da der Slave eigenständig an eine Broadcastadresse sendet, können wir hier nur mit der MAC-Quelladresse und der Verbindungs-ID arbeiten.

- Öffnen Sie im Hauptfenster des Programms mit **Settings > Filter Settings** (3) in die Filtereinstellungen.
- Es öffnet sich das Dialogfenster der Filtereinstellungen, in dem Sie folgende Einstellungen vornehmen.

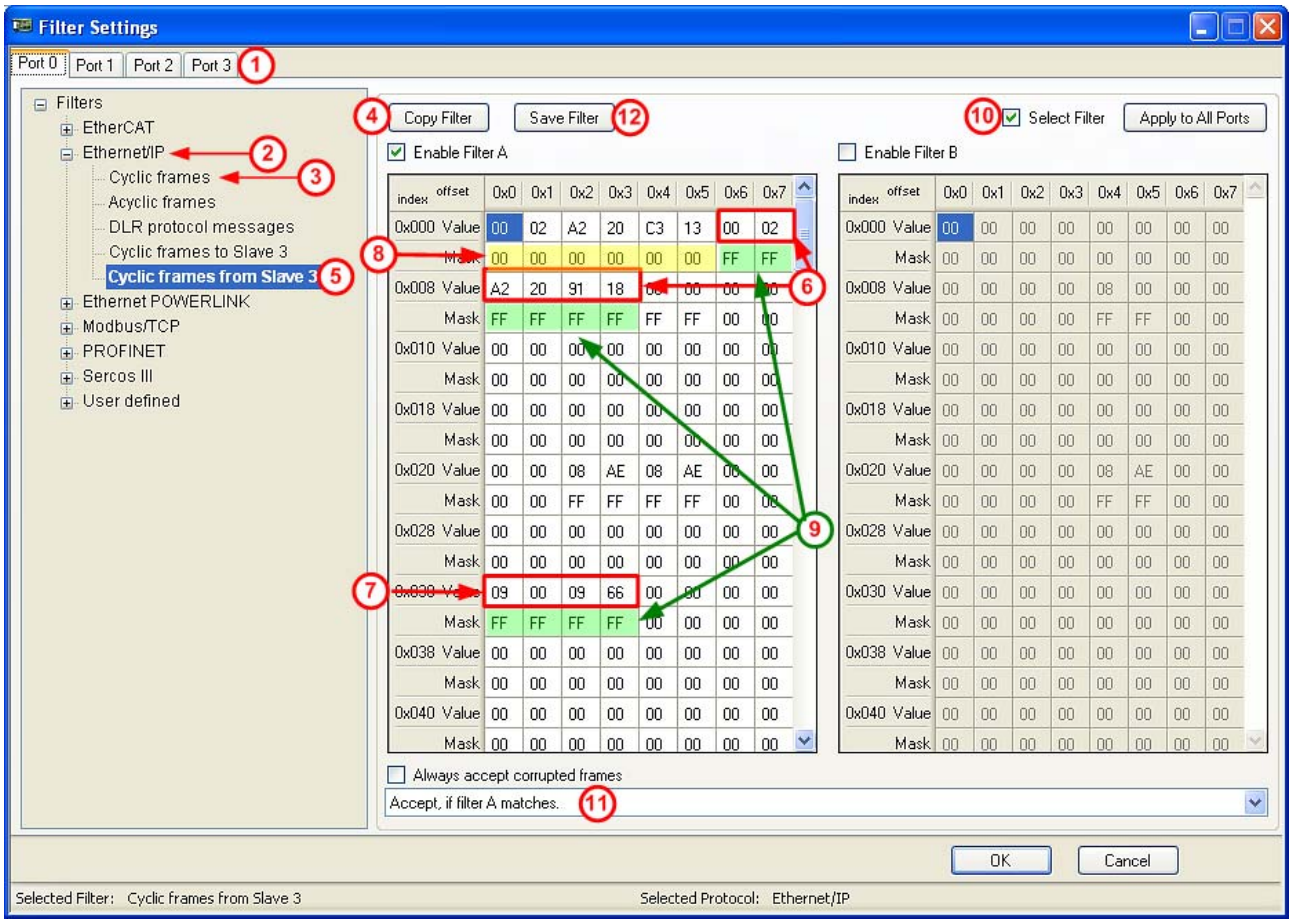


Abbildung 60: EtherNet/IP netANALYZER Filter Slave 3 → cifX

- (1) Wählen Sie den Reiter für den Port aus (auf dem bisher keine Telegramme detektiert wurden), für den Sie den neuen Filter erstellen wollen. (Hier ist es der Port 0, in Ihrer Anwendung kann es ein anderer Port sein.)
- Wählen Sie **Ethernet/IP** (2) **> Cyclic frames** (3).
- Kopieren Sie den Filter mit **Copy Filter** (4).
- Vergeben Sie einen neuen Namen für den Filter. (Hier: **Cyclic frames from Slave 3** (5).)
- Geben Sie die MAC-Adresse des Slave 3 als Quelladresse ein (6).

© Hilscher, 2008-2012

- Geben Sie die identifizierte Verbindungs-ID (7) ein.
  Achtung: Diese ist nach jedem Netzwerkanlauf neu zu ermitteln!
- Füllen Sie die Maskenfelder unter der MAC-Zieladresse mit „**00**“ (8). Dadurch werden diese Datenfelder nicht mehr abgeprüft.
- Füllen Sie die Mask-Felder unter der MAC-Quelladresse und der Verbindungs-ID mit „**FF**“ (9).
- Haken Sie **Select Filter** (10) an.
- Wählen Sie **Accept, if filter A matches** (11) aus (Cyclic frames from Slave 3).
- Speichern Sie den Filter mit **Save Filter** (12).
- Wählen Sie den zweiten Port unter (1) aus, an dem keine Telegramme detektiert wurden (hier Port 2).
- Wählen Sie den soeben erstellten Filter aus.
- Haken Sie **Select Filter** (11) an.
- Prüfen Sie die Einstellungen für alle Ports.
- Verlassen Sie den Filter-Dialog mit **OK** (12).
- Wählen Sie im **Timing Analyse** aus.
- Es öffnet sich im Vordergrund das Fenster zur grafischen Darstellung der Zeitanalyse (Timing Analysis).

Abbildung 61: netANALYZER Timing-Analyse-Fenster

Das Timing Analysis-Fenster unterteilt sich in 4 Unterfenster, die wiederum 2 Teilfenster (Histogramm und Historie) beinhalten. Im weiteren Verlauf dieses Messaufbaus wird in der Regel immer nur ein Unterfenster angesprochen.

Die Größe der Einzelfenster können Sie durch ziehen des Kreuzungspunktes der Fensterteilungslinien verändern.

© Hilscher, 2008-2012

Sie können sich auch nur das Historie- oder Histogramm-Fenster anzeigen lassen. Dieses können Sie im Haupt-Fenster des netANALYZERs unter **Settings > Analysis Configuration** einstellen.

6.3.3 Einstellungen in den Timing-Analysefenstern

Achten Sie darauf, dass in allen Unterfenstern zunächst **Auto Scale** ① eingestellt ist.

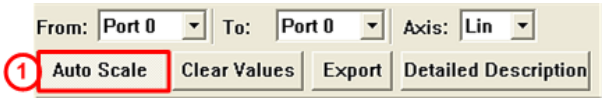


Abbildung 62: netANALYZER Timing-Auto-Scale

Damit stellen Sie sicher, dass (wenn Telegramme detektiert werden) diese auch als Balken sichtbar sind und nicht außerhalb des Zeitstrahls liegen. (Achtung: Der Zeitstrahl geht in dieser Darstellung senkrecht nach oben.)

➢ Stellen Sie die From / To - Bedingungen für jedes Teilfenster wie folgt ein:

Hinweis: Wegen der Autocrossover-Funktionalität. der Ports der netANALYZER-Karte können bei Ihrem Testaufbau. die Telegramme ggf. auch über die entsprechenden korrespondierenden Port laufen. Passen Sie die Ports entsprechend Ihres Aufbaus an.

6.3.3.1 Einstellungen für Teilfenster A

Hier soll die Zykluszeit für Telegramme von der cifX zum Slave 3 ermittelt werden.

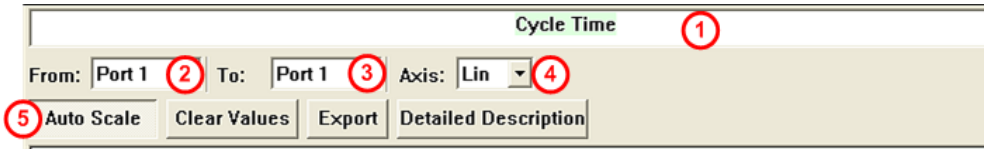


Abbildung 63: EtherNet/IP Porteinstellungen für Zykluszeit, Timingfenster A

➢ Da die Telegramme von der cifX zum Slave 3 (in dem hier dargestellten Versuch) über den Port 1 laufen, ist hier bei **From** ② and **To** ③ der **Port 1** einzustellen.
Bei ① können Sie einen beschreibenden Text für die Messung eingeben.
Achten Sie auf die **Auto Scale** Einstellung ⑤.

6.3.3.2 Einstellungen für Teilfenster B

Hier soll die Durchlaufzeit von Telegrammen der cifX an Slave 3 durch Slave 1 und 2 gemessen werden.

Abbildung 64: EtherNet/IP Porteinstellungen für Antwortzeit Slave 3, Timingfenster B

➢ Da die Telegramme zu Slave 3 über **Port 1** laufen, ist dieser unter **From** ② einzustellen.
Da die Signale zu Slave 3 durch Slave 1 und 2 über den **Port 3** laufen,

© Hilscher, 2008-2012

ist dieser bei **To** ③ einzustellen.

Achten Sie auf die **Auto Scale** Einstellung ⑤.

6.3.3.3 Einstellungen für Teilfenster C

Hier soll die Zykluszeit der Eingangsdaten-Telegramme ins EtherNet/IP-Netzwerk gemessen werden.

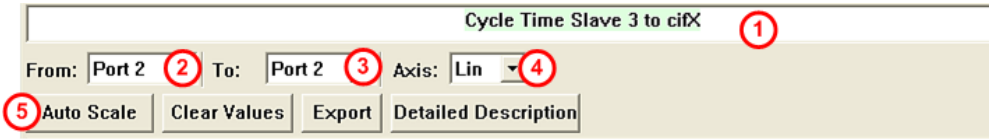


Abbildung 65: EtherNet/IP Porteinstellungen für Durchlaufzeit zum Slave 3, Timingfenster C

➢ Die Telegramme vom Slave 3 laufen in diesem Aufbau über den Port 2. Daher ist für die Zykluszeitmessung bei **From** ② und **To** ③ Port 2 einzustellen.

6.3.3.4 Einstellungen für Teilfenster D

Hier soll die Durchlaufzeit durch Slave 1 und 2 für Signale vom Slave 3 zur PC-Karte cifX gemessen werden.

Abbildung 66: EtherNet/IP Porteinstellungen für Durchlaufzeit durch Slave 1 und 2 zur cifX, Timingfenster D

➢ Da die Telegramme vom Slave 3 zur cifX entsprechend der Analyse der *Abbildung 57* über Port 2 und 0 laufen, ist hier bei **From** ② **Port 2** und **To** ③ **Port 0** einzustellen.

6.3.4 Messungen durchführen

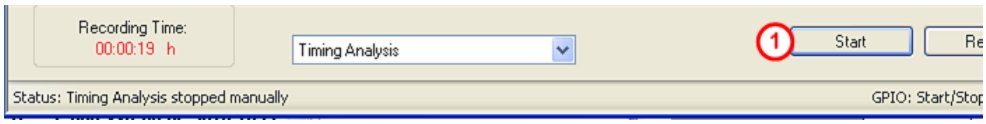


Abbildung 67: Hauptfenster des netANALYZERs

➢ Gehen Sie zurück in das Hauptfenster des netANALYZERs und Starten Sie einen neuen Messzyklus mit **Start** ①.

➢ Sie erhalten folgende Messergebnisse.

© Hilscher, 2008-2012

6.3.4.1 Zykluszeit für den Telegrammweg cifX nach Slave 3

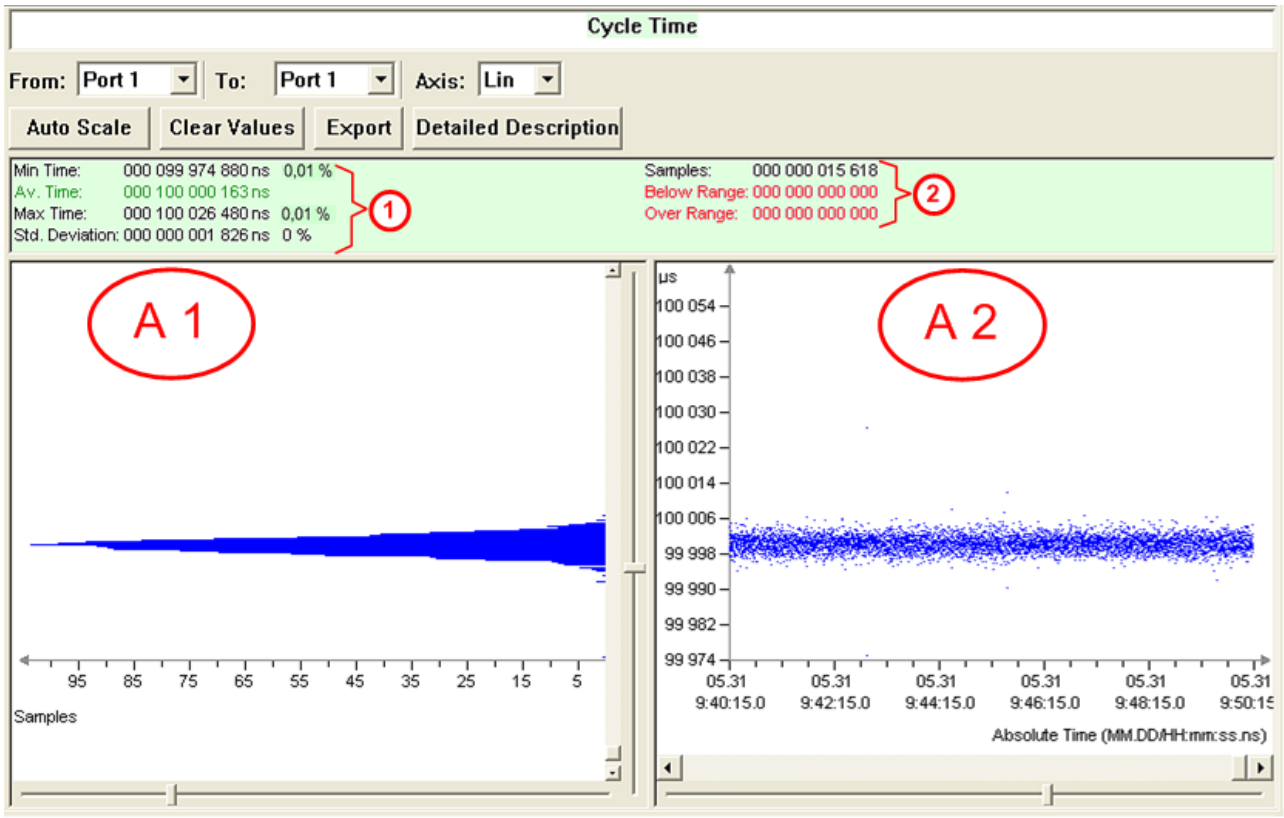


Abbildung 68: EtherNet/IP, Zykluszeit cifX → Slave 3

Im Teilfenster „**A 1**“ ist das Histogramm und im Teilfenster „**A 2**“ die Historie der Telegramme zu sehen.

Ist der **From**- und der **To**-Port identisch, wird immer die Zykluszeit gemessen, unabhängig davon, ob in Richtung des Slaves zum Master oder in Richtung Master zum Slave gemessen wird.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Zykluszeit, sowie die prozentuale Abweichung zur mittleren Zykluszeit.	99,975 ms
Av Time	Die mittlere Durchlaufzeit der Telegramme..	100,000 m s
Max Time	Die maximale Durchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	100,026 ms
Std. Deviation	Die Standardabweichung der Durchlaufzeit.	1,826 µs

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	15618
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

6.3.4.2 Durchlaufzeit (durch Slave 1 und 2) für Telegrame der cifX an Slave 3

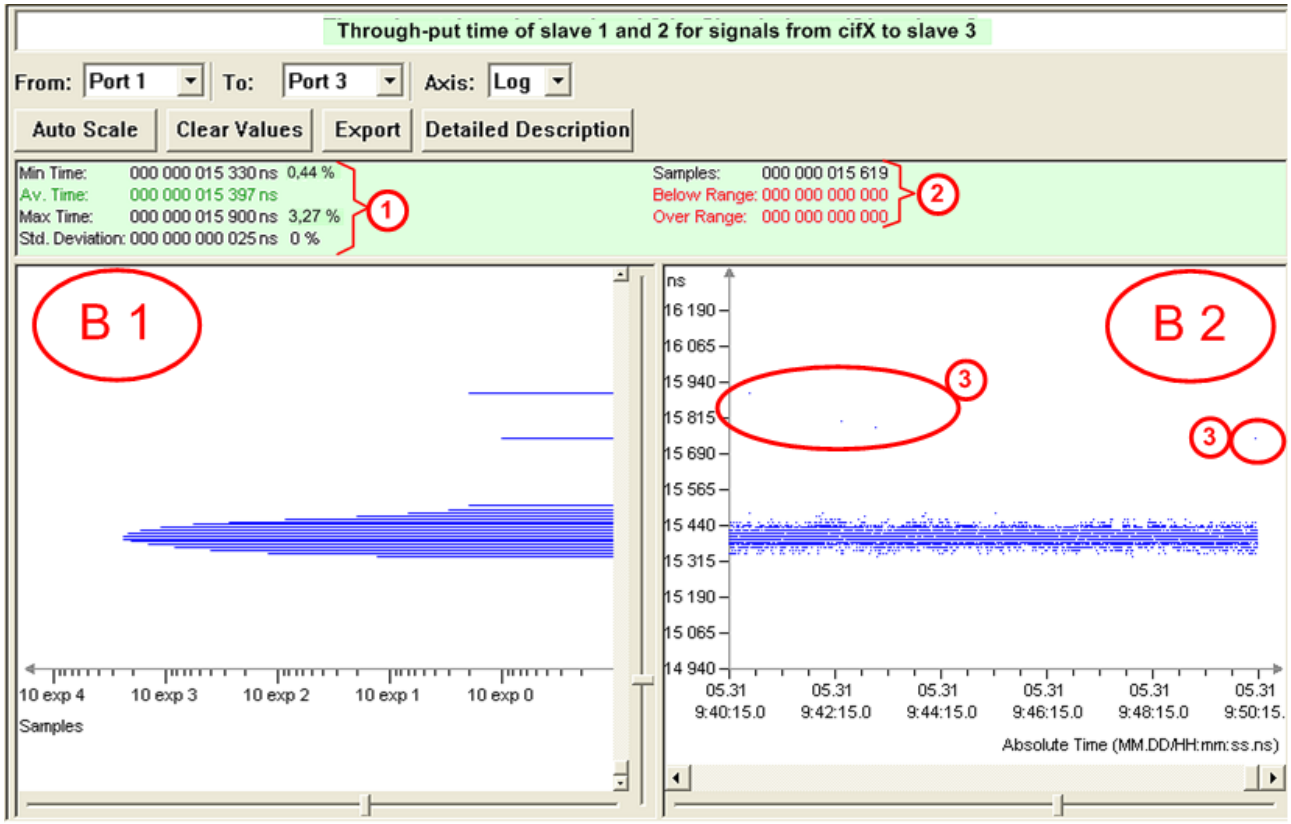


Abbildung 69: EtherNet/IP, Durchlaufzeit cifX -> Slave3 durch Slave 1 und 2

Im Teilfenster „**B 1**“ ist das Histogramm und im Teilfenster „**B 2**“ die Historie der Telegramme zu sehen.

Hier ist zu erkennen, dass die maximale Durchlaufzeit nur von wenigen zeitlich sehr weit auseinander liegende Telegramme ③ bestimmt wird.

Die meisten Telegramme passieren die beiden Slaves hier mit ca. 15,397 µs.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Durchlaufzeit, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	15,330 µs
Av Time	Die mittlere Durchlaufzeit der Telegramme..	15,397 µs
Max Time	Die maximale Durchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	15,900 µs
Std. Deviation	Die Standardabweichung der Durchlaufzeit.	25 ns

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	15619
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

6.3.4.3 Zykluszeit Slave 3

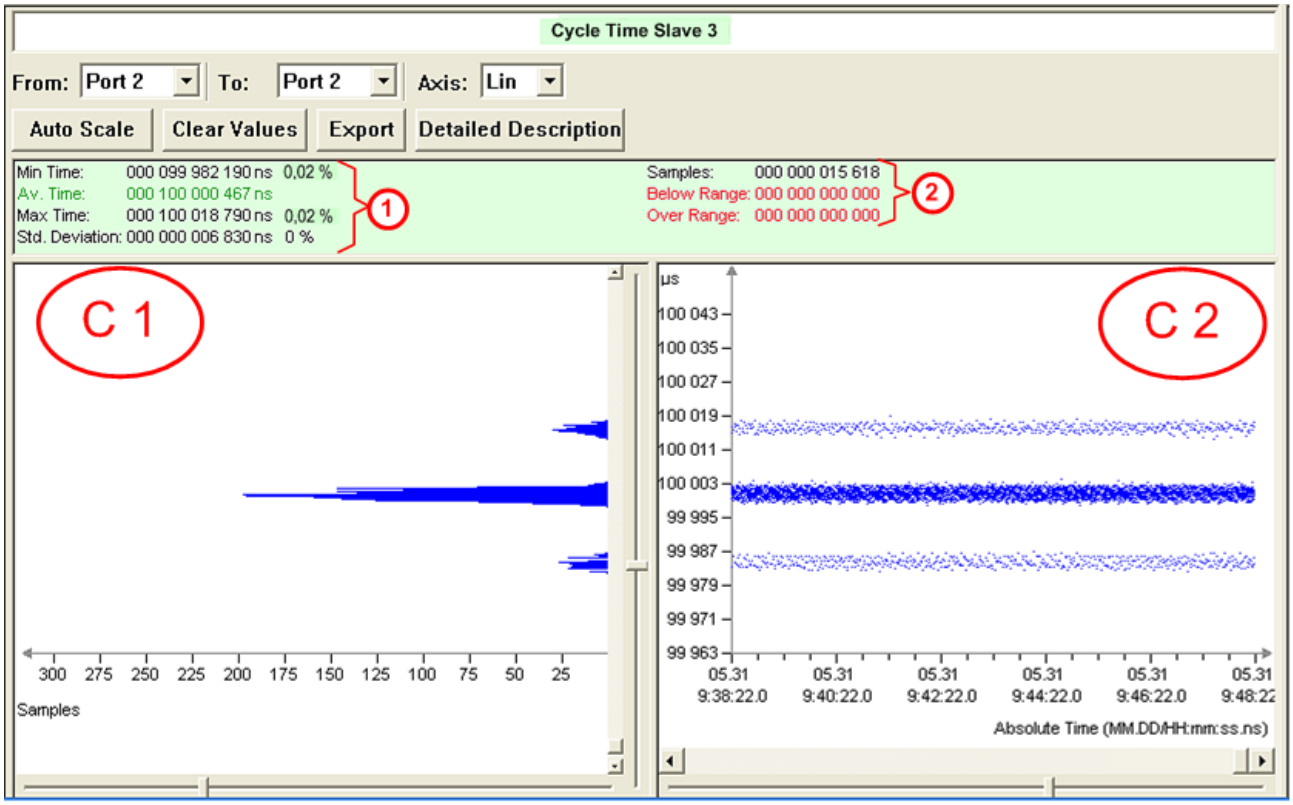


Abbildung 70: EtherNet/IP, Zykluszeit des Slave 3

Im Teilfenster „**C 1**“ ist das Histogramm und im Teilfenster „**C 2**“ die Historie der Telegramme zu sehen.

Hier sind deutlich 2 Nebenspitzen zum Haupttakt zu erkennen. Diese sind folgendermaßen erklärbar.

Der Slave hat eine feste Zykluszeit. Wird diese durch zufällige Ereignisse gestört, wird etwas später im Netzwerk gesendet. Dadurch verkürzt sich aber der Abstand zum nächsten Senden um die vorherige Verzugszeit. Daher tritt immer eine positive und negative Verzugszeit gemeinsam auf, um den absoluten Zyklus beizubehalten.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Zykluszeit, sowie die prozentuale Abweichung zur mittleren Zykluszeit.	99,982 ms
Av Time	Die mittlere Zykluszeit der Telegramme..	100,000 ms
Max Time	Die maximale Durchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	100,018 ms
Std. Deviation	Die Standardabweichung der Zykluszeit.	6,830 µs

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	15618
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

6.3.4.4 Durchlaufzeit Slave 3 nach cifX durch Slave 2 und 1

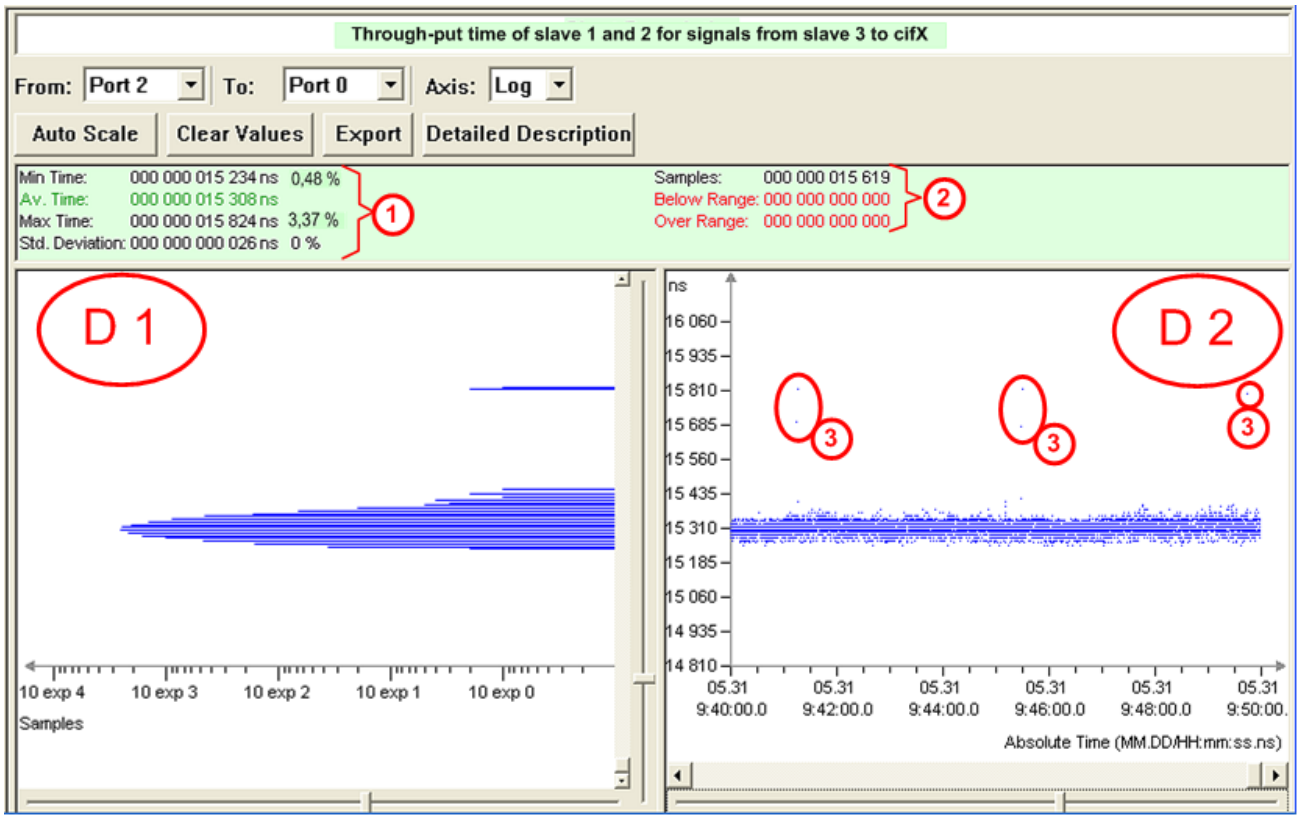


Abbildung 71: EtherNet/IP, Durchlaufzeit Slave 2 und 1 Slave 3 → cifX

Im Teilfenster „**D 1**“ ist das Histogramm und im Teilfenster „**D 2**“ die Historie der Telegramme zu sehen.

Es ist zu erkennen, dass die Durchlaufzeiten der beiden Signalrichtungen leicht unterschiedlich sind.

Es ist zu erkennen, dass die max. Durchlaufzeit durch sehr wenige isolierte Ereignisse ③ verursacht wird.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Durchlaufzeit, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	15,234 µs
Av Time	Die mittlere Durchlaufzeit der Telegramme..	15,308 µs
Max Time	Die maximale Durchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	15,824 µs
Std. Deviation	Die Standardabweichung der Durchlaufzeit.	26 ns

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	15619
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

6.4 Datenaufzeichnungen durchführen

Es sollen die Telegramme der PC-Karte cifX zu den Slaves und die Antworttelegramme von den Slaves an die PC-Karte cifX aufgezeichnet werden.

Voraussetzungen:

- Der Hardware-Aufbau wie unter *Hardware-Aufbau* auf Seite 58 beschrieben muss erstellt sein,
- die Konfiguration für die PC-Karte cifX muss erfolgt sein (siehe Abschnitt 6.4 im Dokument Benutzerhandbuch Real-Time-Ethernet-Kit - Kommunikationssysteme für Real-Time-Ethernet Installation, Bedienung und Konfiguration),
- es muss ein Datenaustausch zwischen der PC-Karte cifX und den Slaves erfolgen.

➢ Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

↬ Sie gelangen ins Hauptfenster des netANALYZERs.

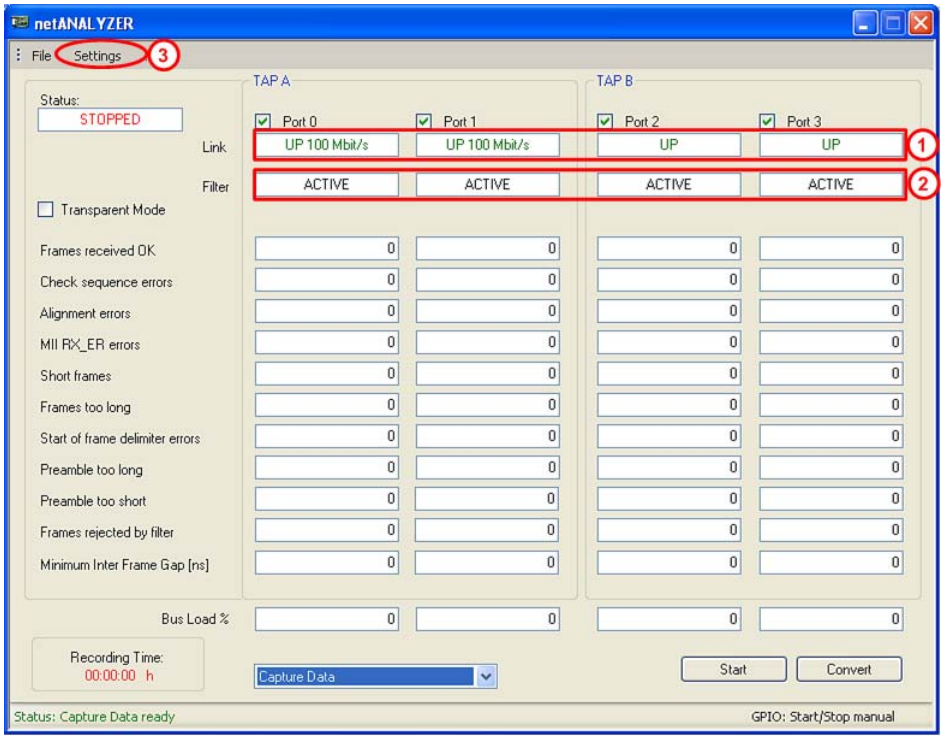


Abbildung 72: netANALYZER Einstiegsfenster

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 58 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP** gekennzeichnet.

➢ Stellen Sie sicher, dass unter dem Dialogweg (wie bei ② dargestellt) **Settings > Filter Settings** die Filtereinstellung aus Abschnitt *Zeitmessung vorbereiten* auf Seite 64 eingestellt sind.

Das später dargestellte Beispiel bezieht sich auf die Filtereinstellungen des Hardware-Aufbaus aus Abschnitt Hardware-Aufbau auf Seite 58.

➢ Verlassen Sie das Dialogfenster der Filtereinstellungen mit **OK**.

© Hilscher, 2008-2012

Sie kommen zurück ins Hauptfenster.

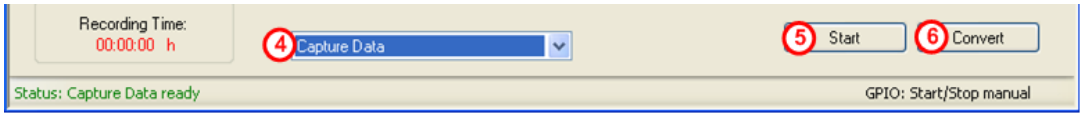


Abbildung 73: Datenaufzeichnung starten

- Stellen Sie sicher, dass **Capture Data** (4) eingestellt ist.
- Klicken Sie **Start** (5), um die Aufzeichnung zu starten.

Die Schaltfläche **Start** (5) wird zur Schaltfläche **Stop** (5).

- Warten Sie bis eine ausreichende Anzahl von Telegrammen aufgezeichnet wurden.
- Klicken Sie **Stop** (5).
- Klicken Sie **Convert** (6).

Es erscheint folgendes Fenster:

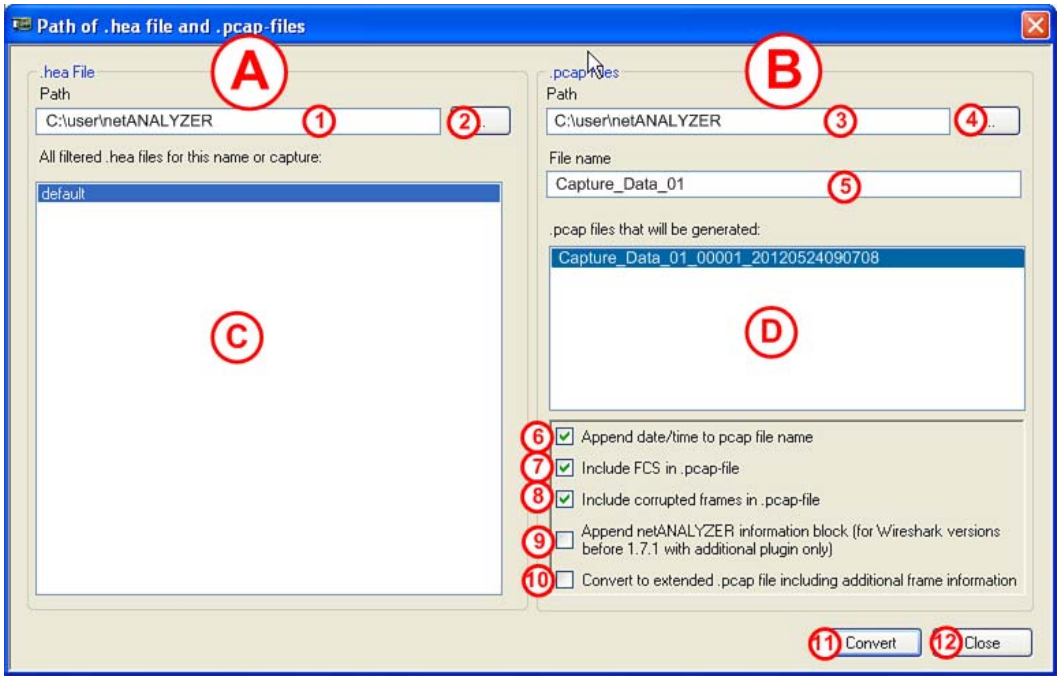


Abbildung 74: pcap-Konvertierung 1

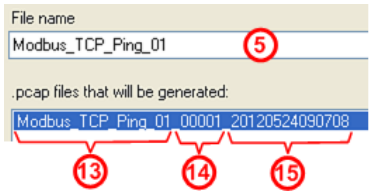
Das obige Fenster teilt sich in zwei Bereiche:

Fensterbereich (A)

Bedienelement	Erläuterung
Path (1)	Vom Bediener auszuwählender Pfad, aus welchem der netANALYZER die Binär-Datei (**.hea*) zur Konvertierung lesen soll. Die hier gemachten Einstellungen wirken sich auch auf die nächsten Datenaufzeichnungen aus. Die Einstellung unter **Settings > File Settings** wird damit verändert.
Schaltfläche (2)	Auswahlschaltfläche zur Auswahl des Quellverzeichnisses der .hea-Dateien.
All filtered .hea files for this name or capture (C)	Anzeigeliste der .hea-Dateien im ausgewähltem Verzeichnis

© Hilscher, 2008-2012

Fensterbereich B

Bedienelement	Erläuterung
Path 3	Der vom Bediener zu definierende Pfad, unter welchem die **netANALYZER**-Software die konvertierte WinPcap-Datei (**.pcap*) ablegen soll.
Schaltfläche 4	Auswahlschaltfläche zur Auswahl des Zielverzeichnis der .pcap-Dateien.
File name 5	Systematische Dateibezeichnung für die **.pcap*-Dateien. Die **netANALYZER**-Software vergibt zusätzlich für jede Datei noch eine fortlaufende Nummer im Dateinamen.
.pcap files that will be generated D	Vorschau der zu erzeugenden **.pcap*-Dateien. Dabei ist der Namensaufbau wie folgt:  13 der unter 5 ausgewählte Dateiname. 14 laufende Zählnummer 15 Zeitinformation, bestehend aus: yyyymmddhhmmss (Beginn der Aufzeichnung der hea-Datei, (nur wenn 6 der Haken gesetzt wurde.).
Append date/time to pcap file name 6	Ist der Haken gesetzt, werden Datum und Zeit im Dateinamen ergänzt.
Include FCS in .pcap-files 7	Checkbox ob die Ethernet-Prüfsumme mit in der PCAP-Datei enthalten sein soll oder nicht. (Einige Wireshark-Dissectoren unterstützen FCS nicht.) **Hinweis:** Wenn **Convert to extended .pcap file including additional frame information** angehakt ist, ist **Include FCS in .pcap-file** ausgegraut, da FCS dann immer in eine .pcap-Datei konvertiert wird. FCS = Frame Check Sequence (Ethernet-Prüfsumme) Nicht auswählbar, wenn Option 10 angehakt, jedoch aktiv.
Include corrupted frames in .pcap file 8	Ist diese Option aktiviert, werden auch fehlerhafte Frames in die .pcap-Datei übernommen. Ist die Option deaktiviert werden nur korrekte Telegramme in der .pcap-Datei gespeichert.
Append netANALYZER information block (for Wireshark versions before 1.7.1 with additional plug in only) 9	Die Option erfordert für Wireshark-Versionen < V1.7.1 die Installation des netANALYZER-Wireshark-Plugins. Fügt den netANALYZER-Info-Block nach dem Ethernet-Frame in die .pcap-Dateien ein. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen. **Hinweis:** Das .pcap-Dateiformat mit dem Info-Block nach dem Ethernet-Frame wird von Wireshark-Versionen ≥ 1.7.1 nicht mehr unterstützt. Nicht auswählbar, wenn Option 10 angehakt.
Convert to extended .pcap file including additional frame information 10	**Hinweis:** Wird dieser Haken gesetzt, kann das mit der netANALYZER-Software V1.4.x.x erzeugte erweiterte .pcap-Dateiformat nur in Wireshark-Versionen ab V1.7.1 geöffnet werden. Ab der Version der netANALYZER-Software V1.4.x.x kann ein erweitertes .pcap-Dateiformat erzeugt werden. Dabei befindet sich der „netANALYZER Info-Block“ in den 4 Bytes vor dem Ethernet-Frame. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen.
Convert 11	Die Konvertierung der Binär-Dateien ins WinPcap-Format wird gestartet.
Close 12	Sie schließen das Fenster ohne eine Konvertierung zu starten.

- Wählen Sie im Fensterbereich A die zu konvertierende Datei aus.
- Ergänzen Sie die notwendigen Einstellungen im Fensterbereich B.
- Klicken Sie auf die Schaltfläche **Convert** 11, um die Daten ins pcap-Format zu konvertieren.

Nach Abschluss des Konvertierungsvorgangs schließt sich das Fenster.

© Hilscher, 2008-2012

- Öffnen Sie die Datei mit Wireshark.
  Wenn das Programm Wireshark korrekt installiert ist, wird mittels eines Doppelklicks auf die .pcap-Datei diese mit Wireshark geöffnet.
- Es werden folgende Daten angezeigt:
- Doppelklick auf die konvertierte Datei (hier c:\Default_001.pcap), oder starten Sie das Programm Wireshark, wählen Sie dann **File > Open** und die Datei aus.
- Das Programm Wireshark zeigt die Daten wie folgt an:

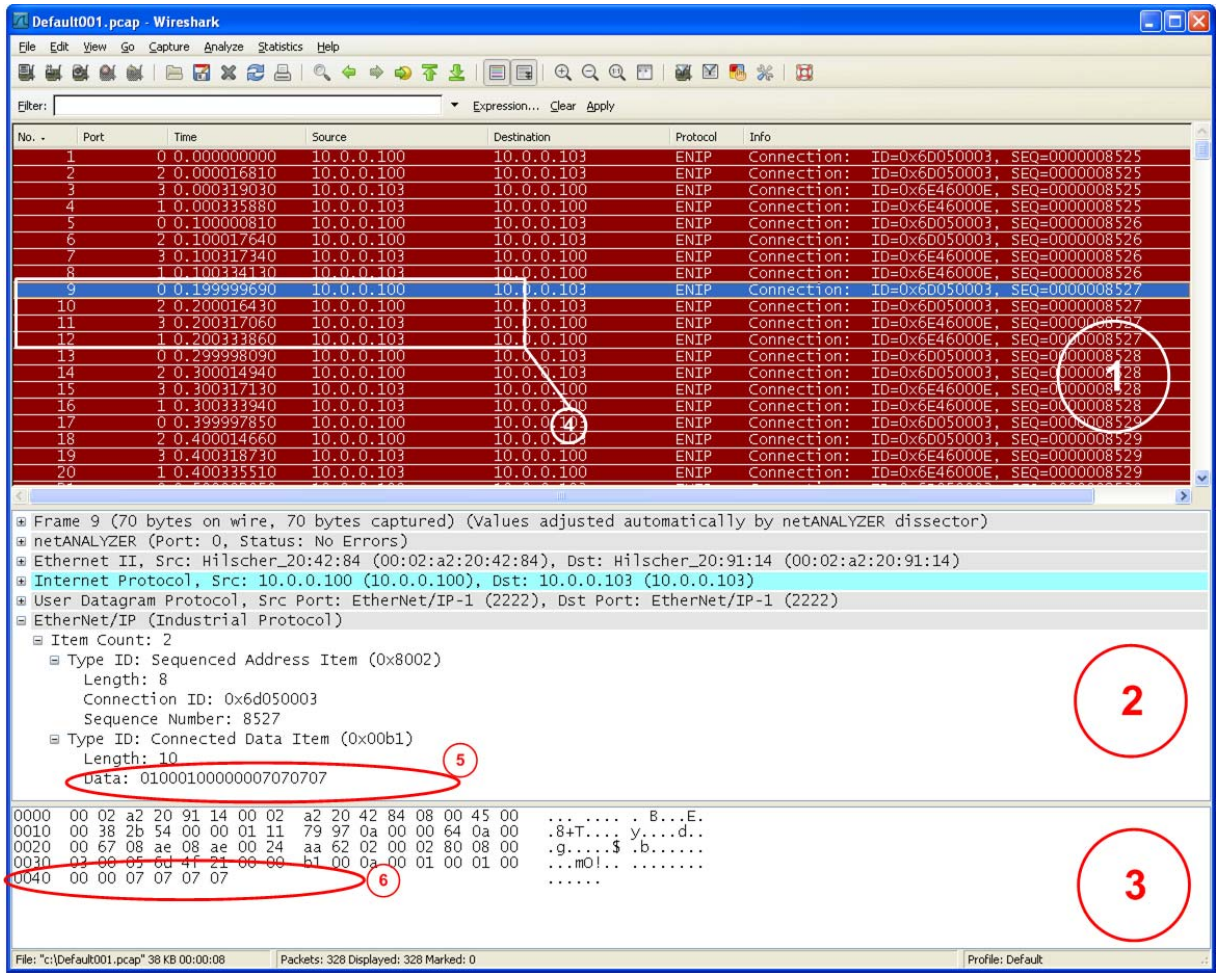


Abbildung 75: EtherNet/IP, Wireshark Telegrammanzeige

① In diesem Fensterbereich sehen Sie die Auflistung jedes Telegramms, welches an jedem Port entsprechend des Filters aufgezeichnet wurde.

② In diesem Fensterbereich können Sie einzelne Telegrammbereiche des ausgewählten Telegramms betrachten.

③ In diesem Fensterbereich werden die Daten des ausgewählten Telegramms auf Byteebene dargestellt.

④ Hier ist ein kompletter Telegrammzyklus des Messaufbaus gekennzeichnet. Die erste Zeile (No 9) enthält das Telegramm wie es vom Master kommt. Dieses wurde am Port 0 aufgezeichnet.

Die zweite Zeile (No 10) enthält das Telegramm nach dem Durchlauf durch Slave 1 und Slave 2 vom Master zum Slave 3.

Die dritte Zeile (No 11) enthält das Telegramm, wie es vom Slave 3 zurück kommt, bevor es zum Slave 2 geht.

Die vierte Zeile (No 12) enthält das Telegramm, wie es vom Slave 3 zurück an den Master kommt, nachdem es Slave 2 und 1 passiert hat.

© Hilscher, 2008-2012

⑤ Hier ist der Teil des Telegramms (erste Zeile des Zyklus) gekennzeichnet, der die Sollwerte für den Slave beinhaltet.

⑥ Hier ist der Teil des Telegramms (erste Zeile des Zyklus) gekennzeichnet, der die Sollwerte für den Slave 3 auf Byteebene beinhaltet.

6.5 Netzlast-Analyse vorbereiten und durchführen

Es soll die Netzlast zwischen Slave 2 und Slave 3 beim Anlauf der Netzwerkkommunikation ermittelt werden und die Belastung durch einen Ping-Aufruf zeigen.

6.5.1 Netzlast-Analyse vorbereiten

Sie können wie in Abschnitt *Datenaufzeichnungen durchführen* auf Seite 76 beschrieben, für den Netzwerkanlauf ein Data-Capture durchführen, um die relevanten Daten für die Einstellungen zu ermitteln oder vordefinierte Filter benutzen.

Wir wollen hier die bereits mitgelieferten Filtereinstellungen verwenden.

6.5.2 Filter einstellen

➢ Hardware-Filter ausschalten

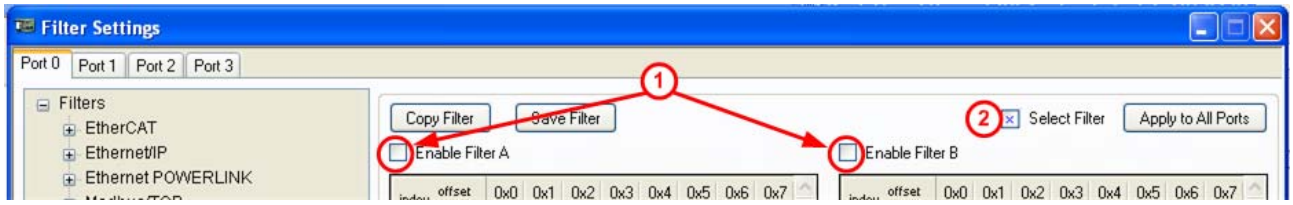


Abbildung 76: Hardware-Filter ausschalten

Hinweis: Die eingestellten Hardware (Standard-Filter) wirken Additiv zu dem *Extended Software Filter*. Aus diesem Grunde entfernen wir die Haken bei Enable Filter ① aus dem Hardware-Filter, oder den Haken bei *Select Filter* ②.

© Hilscher, 2008-2012

➢ Softwarefilter einstellen.

➢ Zur Konfiguration der *Extended Software Filter* gehen Sie wie folgt vor:

1. Wählen Sie im netANALYZER Hauptmenü **Settings > Extended Software Filter Settings**.

Es öffnet sich folgendes Konfigurationsfenster:

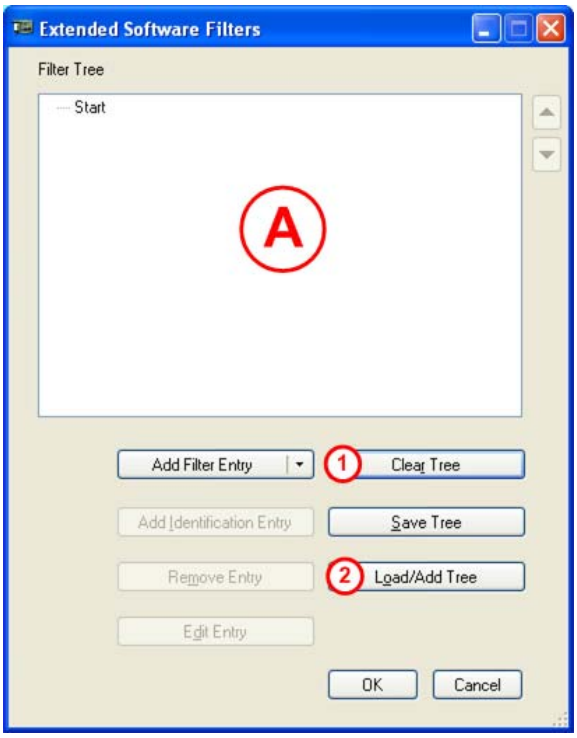


Abbildung 77: Extended Software Filters

➢ Sollte der Bereich nicht so leer sein, wie in der obigen Abbildung dargestellt, klicken Sie **Clear Tree** (1) an, um die Filtereinstellungen zu löschen.

➢ Klicken Sie **Load/Add Tree** (2), um einen Filter auszuwählen.

↬ Es öffnet sich der Dateimanager des Betriebssystems mit dem Verzeichnis der vordefinierten Filter.

➢ Wählen Sie die Datei `EtherNetIP_cyclic_frame.xml` aus. In diesem Filter sind bereits alle Einstellungen für die zyklische Kommunikation an einem Ethernet/IP-Netzwerk vorhanden.

↬ Das Extended Software Filter solle nach dem Aufklappen aller untereinträge wie folgt aussehen.

© Hilscher, 2008-2012

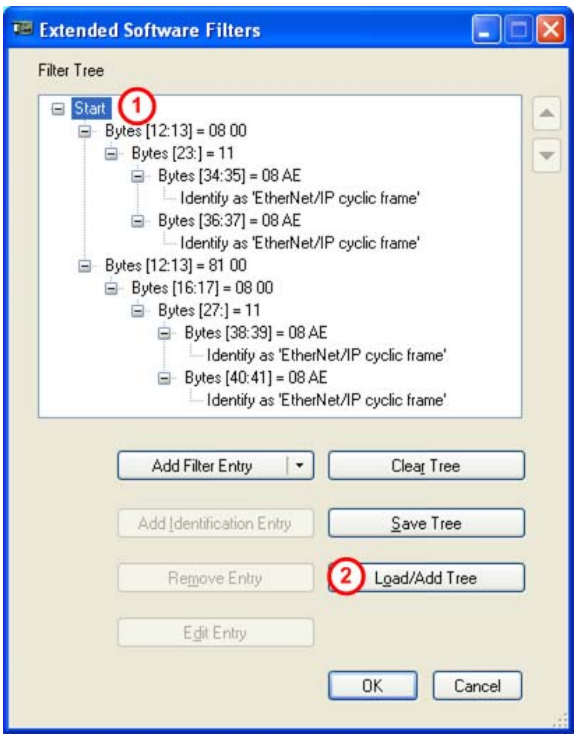


Abbildung 78: Extended Software Filters für zyklische Ethernet/IP Telegramme

Zusätzlich sollen die Ping-Aufrufe auf dem Netzwerk gefiltert werden. Dazu muss dem obigem Filter ein weiterer hinzugefügt werden.

- Markieren Sie den Eintrag **Start** (1) entsprechend der obigen Abbildung um eine ODER-Verknüpfung zu dem bereits ausgewählten Filter zu erzeugen.
- Klicken Sie **Load/Add Tree** (2), um einen weiteren Filter auszuwählen.
- Es öffnet sich der Dateimanager des Betriebssystems mit dem Verzeichnis der vordefinierten Filter.
- Wählen Sie die Datei `ICMP_frame.xml` aus. In diesem Filter sind auch die Einstellungen für einen Ping-Aufruf enthalten.
- Das Extended Software Filter solle nach dem Aufklappen aller untereinträge jetzt wie folgt aussehen.

© Hilscher, 2008-2012

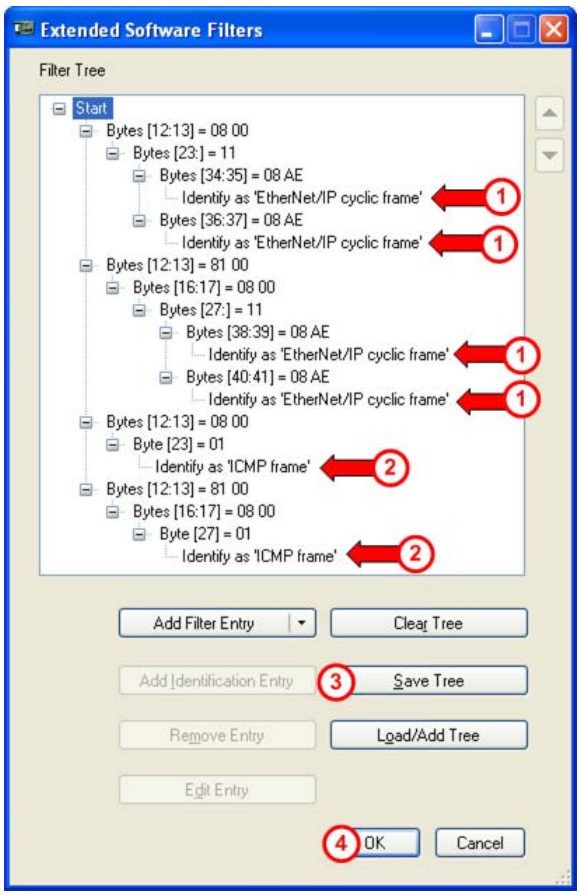


Abbildung 79: Extended Software Filters für zyklische Ethernet/IP-Telegramme und Ping

Für jeden Eintrag mit **Identify as** wird ein Zählertopf für die Analyse eröffnet. Da der Name **Identify as Ethernet/IP cyclic frame** (1) vier mal vorkommt, werden alle diese Filterergebnisse in dem selben Zähltopf gezählt. Dieses gilt ebenso für den Zähltopf **Identify as ICMP frame** (2) (für die Ping-Aufrufe), der zwei Quellen hat.

Hinweis: Treten bei der Telegrammanalyse noch andere Datensätze auf, die nicht den Filterbedingungen entsprechen, wird der Analyse automatisch der Topf „Other” hinzugefügt.

- Speichern Sie die Filtereinstellungen für spätere Anwendungen. Verlassen Sie mit **OK** (3) das Filterfenster.

Sie gelangen zurück in das Hauptfenster des netANALYZERs.

© Hilscher, 2008-2012

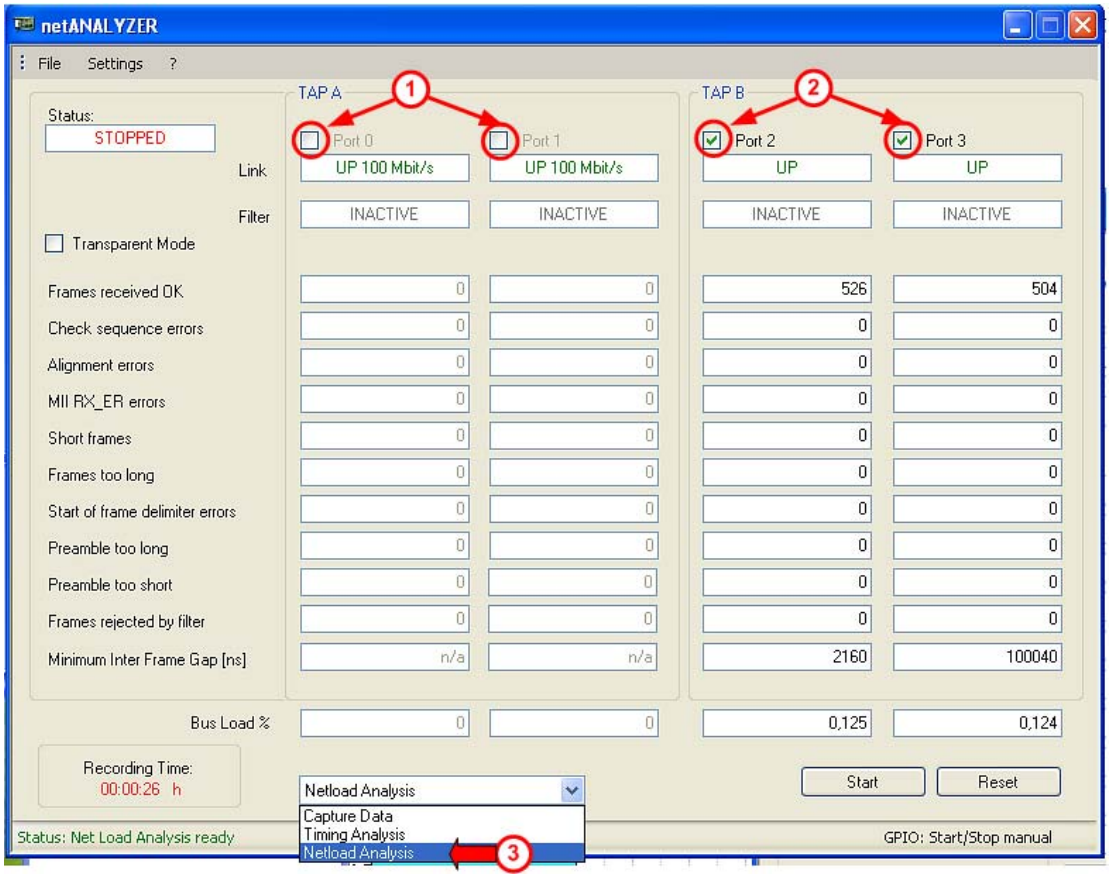


Abbildung 80: netANALYZER Hauptfenster Ethernet/IP Netload Analyse

- Setzen Sie den Haken bei TAP B für Port 2 und Port 3 (2).
  Dieses ist erforderlich, da wegen der Auto Cross Over Funktionalität der Ethernetanschlüsse nicht vorhersehbar ist, über welchen Port die Kommunikation startet.
- Entfernen Sie ggf. die Haken bei TAP A (1), damit die Telegramme nicht doppelt aufgezeichnet werden.

6.5.3 Netzlast-Messung durchführen

- Wählen Sie für die Analyse **Netload Analysis** (3) aus.
- Es öffnet sich das Netload Analysis Fenster.
- Öffnen Sie die Ethernetverbindung am CH 0 des Slave 1 der Abbildung 52 um sie nach dem Start der Analyseaufzeichnung wieder schließen zu können, damit die nicht zyklischen EtherNet/IP-Telegramme bei Verbindungsaufbau erfasst werden können.
- Wählen Sie das Hauptfenster des netANALYZER an.
- Klicken Sie **Start**.
- Die Datenaufzeichnung beginnt.
- Schließen Sie das Kabel am CH 0 des Slaves wieder an.
- Stoppen Sie nach einiger Zeit der Aufzeichnung mit **Stop** im Hauptfenster des netANALYZERs.
- Im Netload Analysis Fenster sehen Sie jetzt etwa folgende Informationen:

© Hilscher, 2008-2012

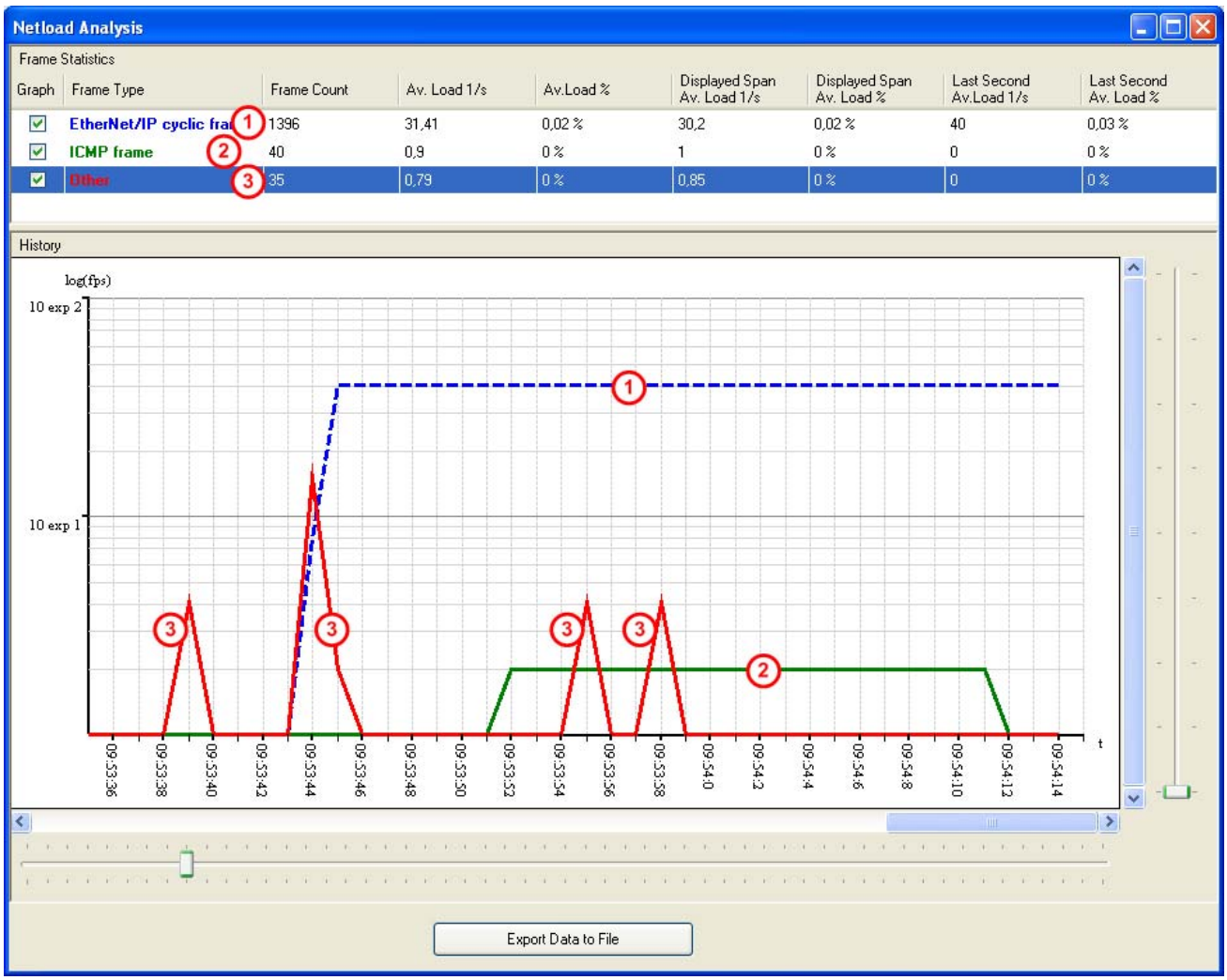


Abbildung 81: Netzlast für zyklische Ethernet/IP Telegramme (Anlauf) und Ping

In der obigen Abbildung ist zu sehen, dass es nach einer Netzunterbrechung zu Beginn der Kommunikation zunächst einige nicht Ethernet/IP-Telegramme (Kurve 3) gibt und die Ethernet/IP-Kommunikation (Kurve 1) ca. 5 sec. nach Behebung der Unterbrechung beginnt.

Die Ping-Aufrufe wurden am CH 1 des Slave 3 eingespeist und waren an den Slave 1 adressiert. Der Ping-Aufruf wurde 20 mal wiederholt (Kurve 2).

Wird die Ethernet/IP-Kommunikation nicht durch Netzwerkunterbrechung neu gestartet, sondern durch eine Spannungswiederkehr der Slaves, ist die nicht Ethernet/IP-Kommunikation vor dem Start der selbigen noch umfangreicher, da dann noch die Kommunikation für die Adressverteilung über den DHCP-Server dazukommt. Dieser Fall wird in der folgenden Abbildung dargestellt.

© Hilscher, 2008-2012

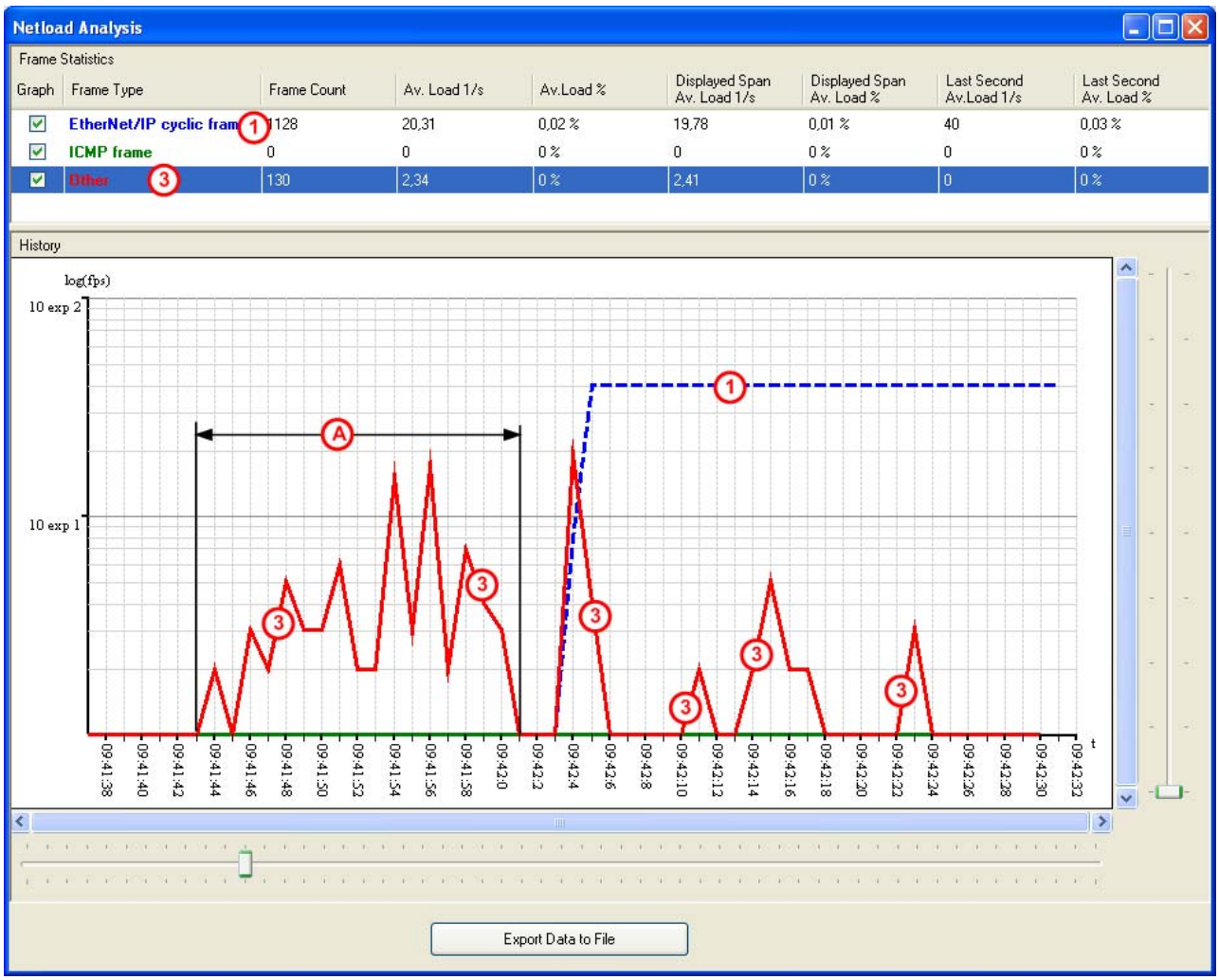


Abbildung 82: Netzlast für zyklische Ethernet/IP Telegramme (Anlauf nach Spannungswiederkehr)

In der obigen Abbildung kommen die nicht Ethernet/IP-Telegramme im Zeitraum (A) überwiegend von der Adresszuteilung der Slaves über den DHCP-Server und dem Test auf identische Adressen im Netzwerk. Der Start der zyklischen Ethernet/IP-Kommunikation erfolgt ca. 16 sec. nach der Spannungswiederkehr. Sind mehr Teilnehmer im Netzwerk vorhanden, wird sich dieser Zeitabschnitt noch vergrößern.

© Hilscher, 2008-2012

7 sercos Analyse

Beispielhaft werden hier folgende Messungen durchgeführt:

- Messung der Ringdurchlaufzeit des Primärrings,
- Messung der ConClk-Zykluszeit am Slave 1,
- Messung der Zykluszeit des Master-Datentelegramms am Ausgang des Masters,
- Messung der Zykluszeit des Master Datentelegramms nach Durchlauf von 3 Slaves.

7.1 Hardware-Aufbau

Für diese Beispielmessung wird folgender Hardware-Aufbau benötigt.

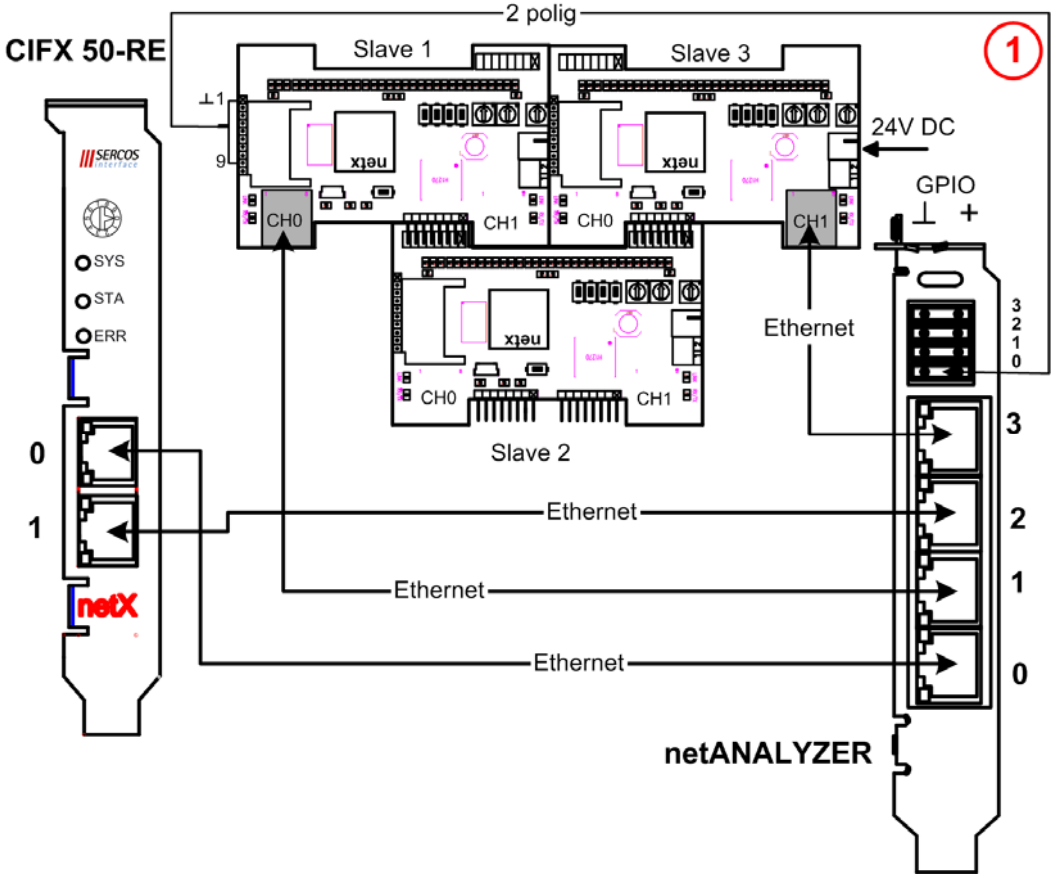


Abbildung 83: sercos, Hardware-Aufbau

Neben den Ethernetverbindungen ist im obigem Beispiel eine 2-polige Leitung (1) vom ConClk-Anschluss (GND Pin 1 und ConClk Pin 9) vom Slave 1 zum GPIO-Anschluss 0 der netANALYZER-Karte zu legen.

Hinweis: Die Einstellungen für die PC-Karte cifX und die NXIO 50 Boards entsprechend Abschnitt 6.5 der Installation, Bedienung und Hardwarebeschreibung dieses Kits müssen vorgenommen worden sein.

© Hilscher, 2008-2012

7.2 Zeitmessung vorbereiten und durchführen

Hinweis: Die PC-Karte cifX und die NXIO-Boards verfügen über eine Autocrossover-Funktionalität. Daher ist ein vertauschen der Kabel am netANALYZER am TAP A (Port 0 und Port 1) sowie am TAP B (Port 2 und Port 3) ohne Bedeutung. Somit sind auch bei der Anzeige der Analysewerte die Portbezeichnungen 0/1 bzw. 2/3 als vertauschbar zu betrachten.

Hinweis: Hier sind nur die für diesen Messaufbau unmittelbar erforderlichen Einstellungen des netANALYZERs beschrieben. Detaillierte Informationen über die Einstell- und Aufzeichnungsmöglichkeiten der Software entnehmen Sie bitte der Dokumentation *Benutzerhandbuch netANALYZER.*

7.2.1 Zeitmessung vorbereiten

Es soll die Ringdurchlaufzeit des Primärrings und die ConClk-Zykluszeit am Slave 1 gemessen werden.

- Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

Sie gelangen in das Hauptfenster des netANALYZERs.

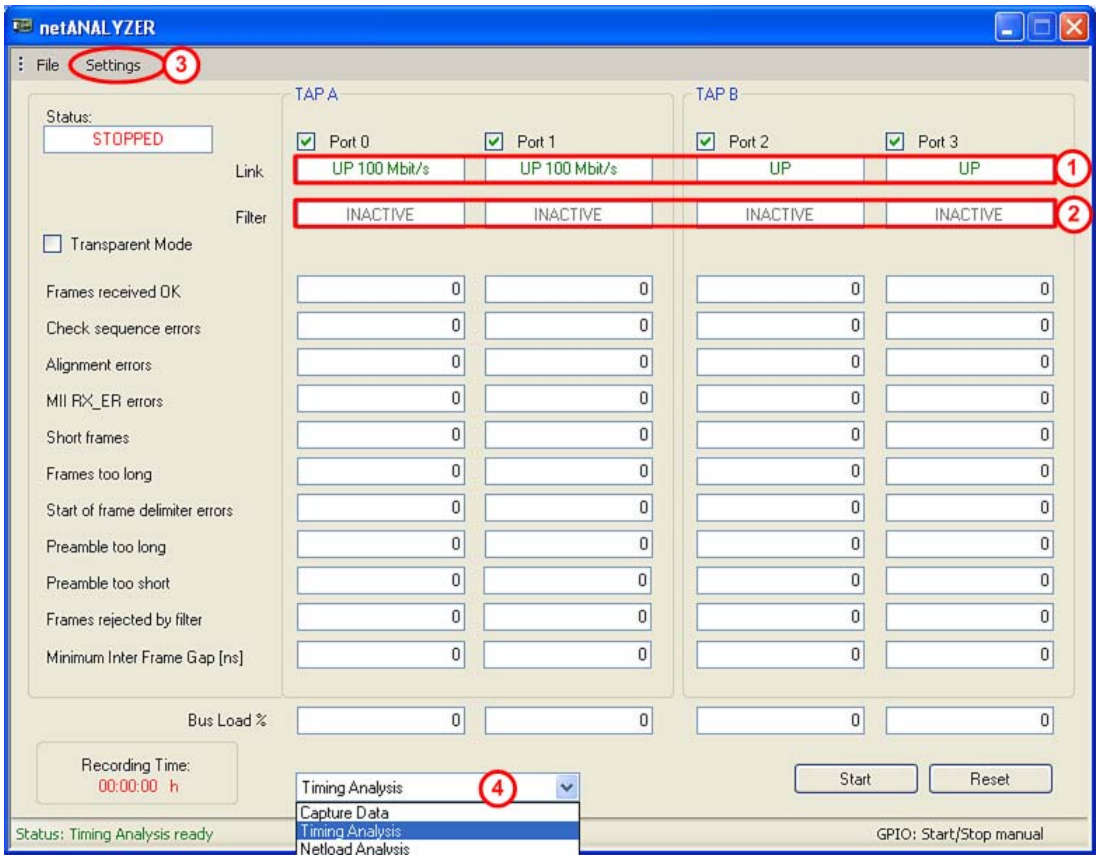


Abbildung 84: netANALYZER Einstiegsfenster

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* Seite 87 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP mit Datenrate** oder bei älteren netANALYZER-Karten bei TAP B nur mit **UP** gekennzeichnet.

In der Zeile ② können Sie sehen, dass derzeit kein Filter aktiv ist.

© Hilscher, 2008-2012

7.2.2 Filter einstellen

➢ Machen Sie unter dem Dialog **Settings > Filter Settings** ③ folgende Einstellungen:

↬ Es öffnet sich das Filtereinstellungsfenster.

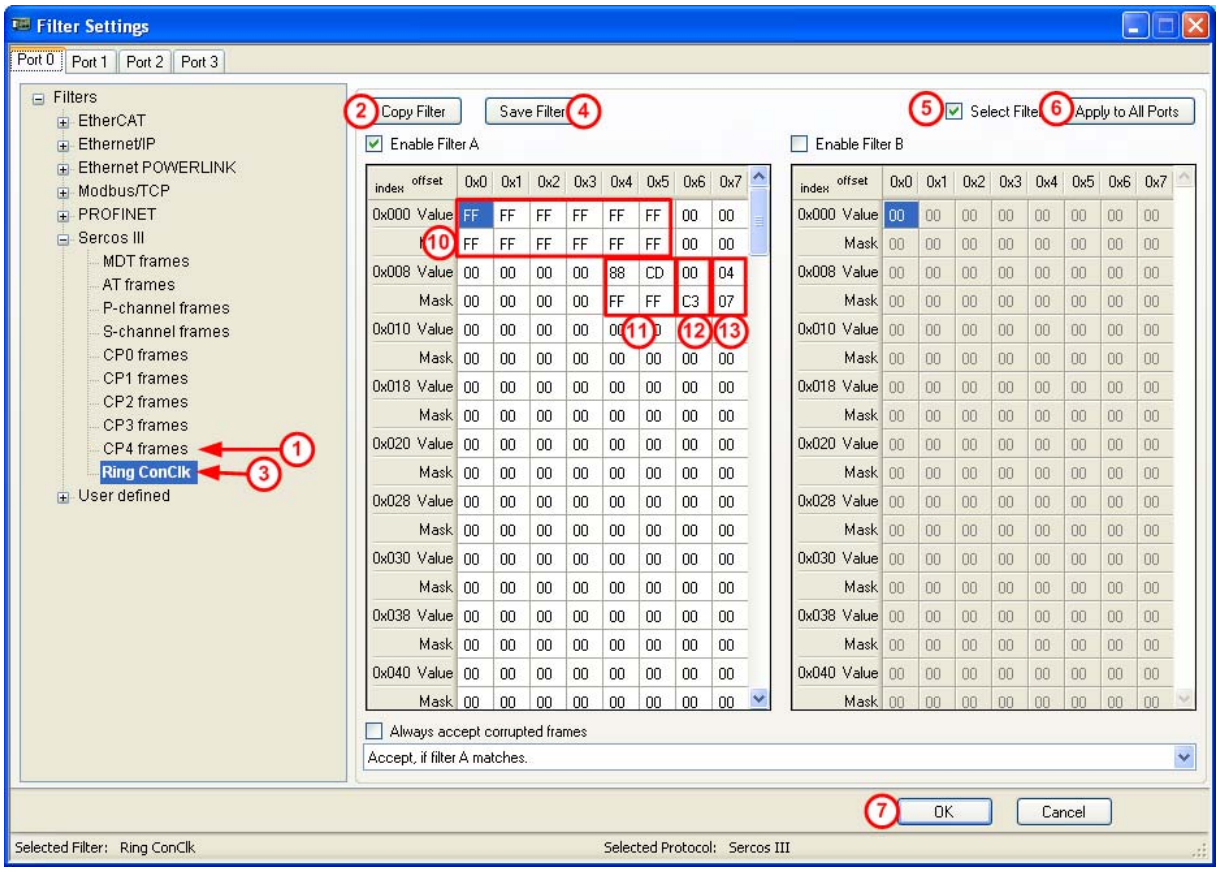


Abbildung 85: netANALYZER Sercos Filtereinstellungen

Gehen Sie zur Filtereinstellung wie folgt vor:

➢ Wählen Sie aus den vordefinierten Filtern den **Filter > Sercos III > CP4 Frames** ① aus.

➢ Klicken Sie **Copy Filter** ②.

➢ Vergeben Sie einen Namen für den kopierten Filter, hier **Ring ConClk.** ③.

➢ Nehmen Sie die Einstellungen vor, wie Sie in der obigen Abbildung in den rechteckigen Kästchen dargestellt sind.

Hierbei bedeuten:

Multicastadresse ⑩, Sercos III Protokoll ⑪, MDT0 primär ⑫, CP4 ⑬.

➢ Speichern Sie die Einstellung mit **Save Filter** ④.

➢ Wählen Sie das Filter für diesen Port aus, indem Sie das Kästchen **Select Filter** ⑤ anklicken.

➢ Klicken Sie **Apply to All Ports** ⑥, damit diese Filtereinstellungen für alle Ports wirksam werden.

➢ Verlassen Sie den Dialog mit **OK** ⑦.

↬ Sie gelangen in das Hauptfenster des netANALYZERs.

➢ Machen Sie unter **Settings > GPIO Settings** folgende Einstellungen:

© Hilscher, 2008-2012

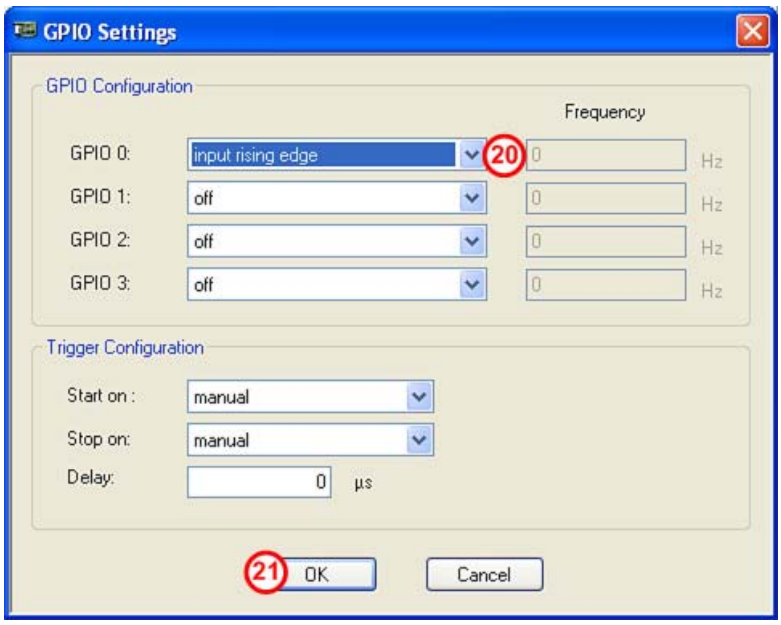


Abbildung 86: netANALYZER Sercos GPIO Settings

- ➢ Stellen Sie GPIO 0 auf **input rising edge** (20) ein.
- ➢ Verlassen Sie den Dialog mit **OK** (21).
- ↬ Sie gelangen in das Hauptfenster des netANALYZERs.
- ➢ Wählen Sie **Timing Analysis** (2).
- ↬ Es öffnet sich im Vordergrund das Fenster zur grafischen Darstellung der Timing Analyse.

Abbildung 87: netANALYZER Timing-Analyse-Fenster

Das Timing Analysis-Fenster unterteilt sich in 4 Unterfenster, die wiederum 2 Teilfenster (Histogramm und Historie) beinhalten. Im weiteren Verlauf dieses Messaufbaus wird in der Regel immer nur ein Unterfenster angesprochen.

© Hilscher, 2008-2012

Die Größe der Einzelfenster können Sie durch ziehen des Kreuzungspunktes der Fensterteilungslinien verändern.

Sie können sich auch nur das Historie- oder Histogramm-Fenster anzeigen lassen. Dieses können Sie im Haupt-Fenster des netANALYZERs unter **Settings > Analysis Configuration** einstellen.

7.2.3 Einstellungen in den Timing-Analysefenstern

Achten Sie darauf, dass in allen Unterfenstern zunächst **Auto Scale** (1) eingestellt ist.

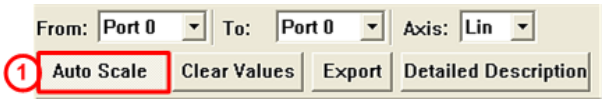


Abbildung 88: netANALYZER Timing-Auto-Scale

Damit stellen Sie sicher, dass (wenn Telegramme detektiert werden) diese auch als Balken sichtbar sind und nicht außerhalb des Zeitstrahls liegen. (Achtung: Der Zeitstrahl geht in dieser Darstellung senkrecht nach oben.)

➢ Stellen Sie die From / To - Bedingungen für jedes Teilfenster wie folgt ein:

Hinweis: Wegen der Autocrossover-Funktionalität. der Ports der netANALYZER-Karte können bei Ihrem Testaufbau. die Telegramme ggf. auch über die entsprechenden korrespondierenden Port laufen. Passen Sie die Ports entsprechend Ihres Aufbaus an.

7.2.3.1 Einstellungen für Teilfenster A

Hier soll die Ringdurchlaufzeit gemessen werden.

➢ Starten Sie kurzzeitig die Timing Analysis. Unter TAP A und TAP B wird sich jeweils ein Port mit Telegrammen füllen.

➢ Hier ergab sich folgendes Bild:

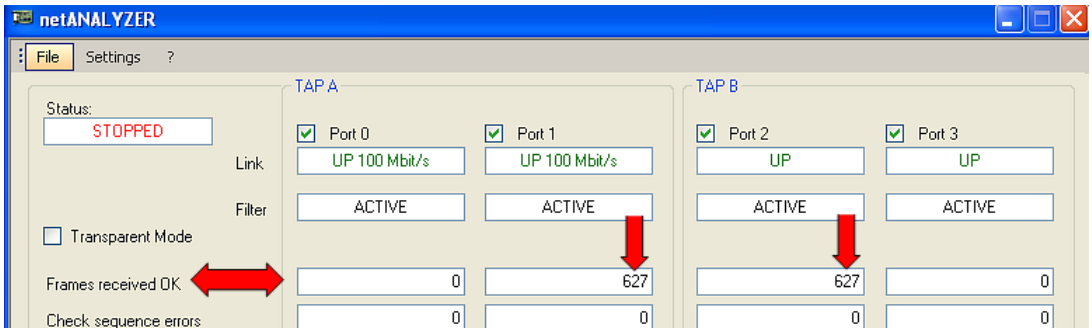


Abbildung 89: netANALYZER Port-Selektion

Hier ist ersichtlich, dass die Telegramme am Port 1 aus der cifX kommen, und über Port 2 zur cifX zurücklaufen.

➢ Nehmen Sie im Fenster A folgende Einstellungen, zur Messung der Ringdurchlaufzeit, vor.

Abbildung 90: Sercos Einstellungen Timinganalysefenster A

© Hilscher, 2008-2012

- In dieser Zeile können Sie eine beliebige Bezeichnung für diese Messung eingeben (1).
- Unter **From:** wählen Sie **Port 1** (2) aus.
- Unter **To:** wählen Sie **Port 2** (3) aus.

Mit dieser Einstellung wird die Zykluszeit der (mittels des Filters selektierten) Telegramme vom Master zum Slave gemessen.

- Hier kann die Skalierung der X-Achse (Anzahl Telegramme) im Teilbild Histogramm zwischen linear und logarithmisch umgeschaltet werden (4).
- Achten Sie darauf, dass **Auto Scale** (5) eingestellt ist, damit die Messergebnis immer im sichtbaren Bereich des Fensters liegen.

7.2.3.2 Einstellungen für Teilfenster B

Messung des ConClk-Zykluses am Slave 1

Abbildung 91: Sercos Einstellungen Timinganalysefenster B

- Unter **From:** wählen Sie **GPIO 0** (2) aus.
- Unter **To:** wählen Sie **GPIO 0** (3) aus.

Mit dieser Einstellung wird der ConClk-Zyklus am Slave 1 gemessen.

- Achten Sie darauf, dass für die Zeitachse **Auto Scale** (5) eingestellt ist.

7.2.3.3 Einstellungen für Teilfenster C

Messung des Zyklus des Masterdatentelegramms am Ausgang des Masters.

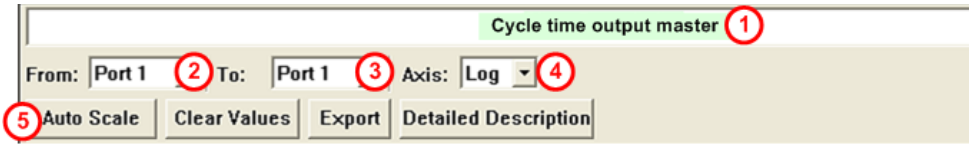


Abbildung 92: Sercos Einstellungen Timinganalysefenster C

- Unter **From:** wählen Sie **Port 1** (2) aus.
- Unter **To:** wählen Sie **Port 1** (3) aus.

Mit dieser Einstellung wird der Zyklus des Masterdatentelegramms am Ausgang des Masters gemessen.

- Achten Sie darauf, dass für die Zeitachse **Auto Scale** (5) eingestellt ist.

7.2.3.4 Einstellungen für Teilfenster D

Messung des Zyklus des Masterdatentelegramms nach Durchlauf von 3 Slaves.

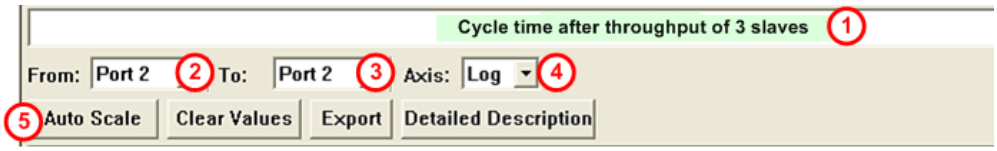


Abbildung 93: Sercos Einstellungen Timinganalysefenster D

- Unter **From:** wählen Sie **Port 2** (2) aus.

© Hilscher, 2008-2012

➢ Unter **To:** wählen Sie **Port 2** ③ aus.

Mit dieser Einstellung wird der Zyklus des Masterdatentelegramms nach dem Durchlauf von 3 Slaves gemessen.

➢ Achten Sie darauf, dass für die Zeitachse **Auto Scale** ⑤ eingestellt ist.

7.2.4 Messung durchführen

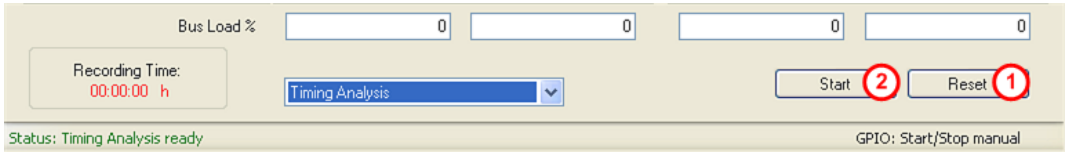


Abbildung 94: netANALYZER Start Analysezyklus

➢ Klicken Sie im Hauptfenster des netANALYZERs **Reset** ①. Damit werden die bisher aufgezeichneten Zeit-Daten gelöscht.

➢ Klicken Sie **Start** ② um die Analyse zu starten.

↬ Die Schaltfläche **Start** wird zur Schaltfläche **Stop**.

➢ Warten Sie die Zeit, in der Sie Telegramme auswerten möchten.

➢ Klicken Sie **Stop**.

7.2.4.1 Timing-Analyse-Fenster A: Ringdurchlaufzeit

Im Fenster A des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

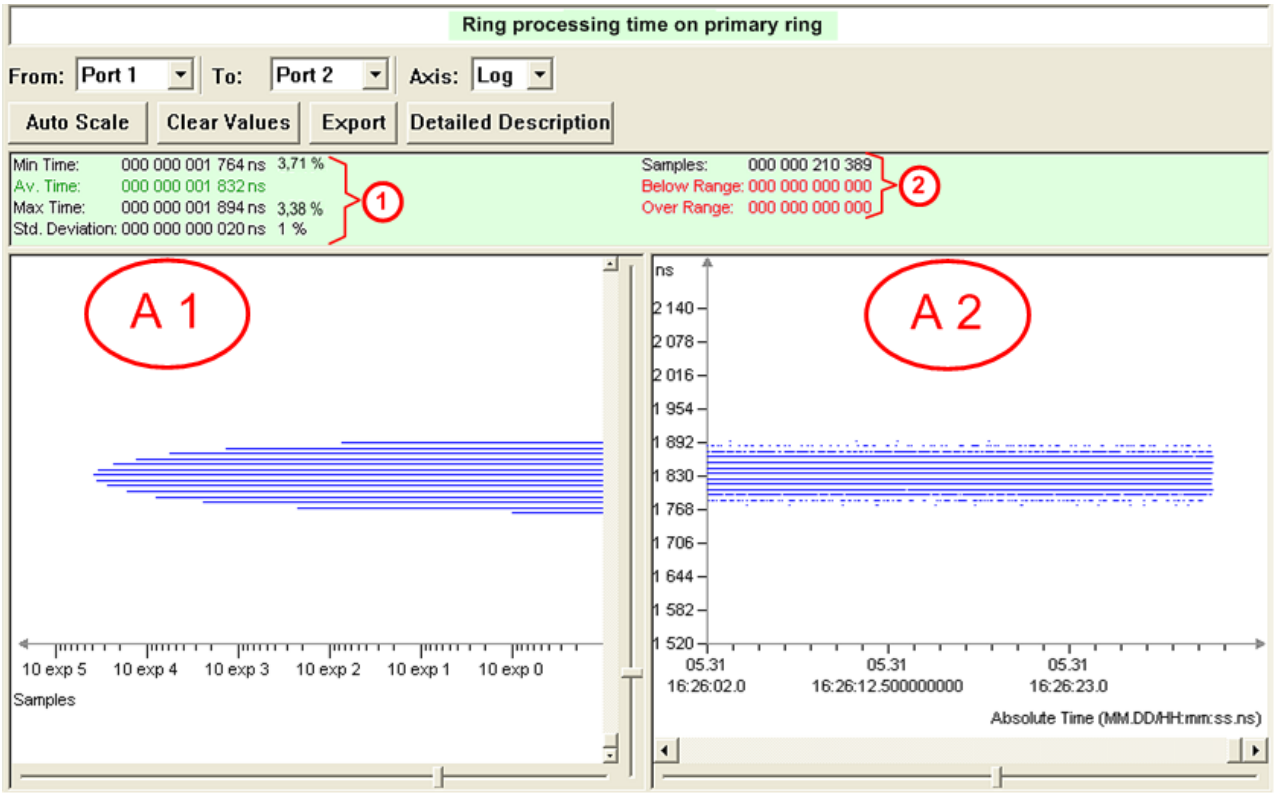


Abbildung 95: netANALYZER Ring-Delay Zeit

Im Fenster „**A 1**“ (dem Histogramm) sieht man die zeitliche Verteilung der einzelnen Telegramme und deren Anzahl.

Im Fenster „**A 2**“ (der Historie) sieht man die Verteilung der Telegramme über die Zeit.

© Hilscher, 2008-2012

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Ring-Durchlaufzeit, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	1,764 µs
Av Time	Die mittlere Ring-Durchlaufzeit der Telegramme..	1,832 µs
Max Time	Die maximale Ring-Durchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	1,894 µs
Std. Deviation	Die Standardabweichung der Durchlaufzeit.	20 ns

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	210389
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

7.2.4.2 Timing-Analyse-Fenster B: ConClk Zykluszeit Slave 1

Im Fenster B des Zeitanalysefensters finden Sie jetzt folgende Informationen:

Anmerkung: Die ConClk-Zeit ist abhängig von der beim Master eingestellten Zykluszeit. Die Zykluszeit wurde auf 2 ms eingestellt.

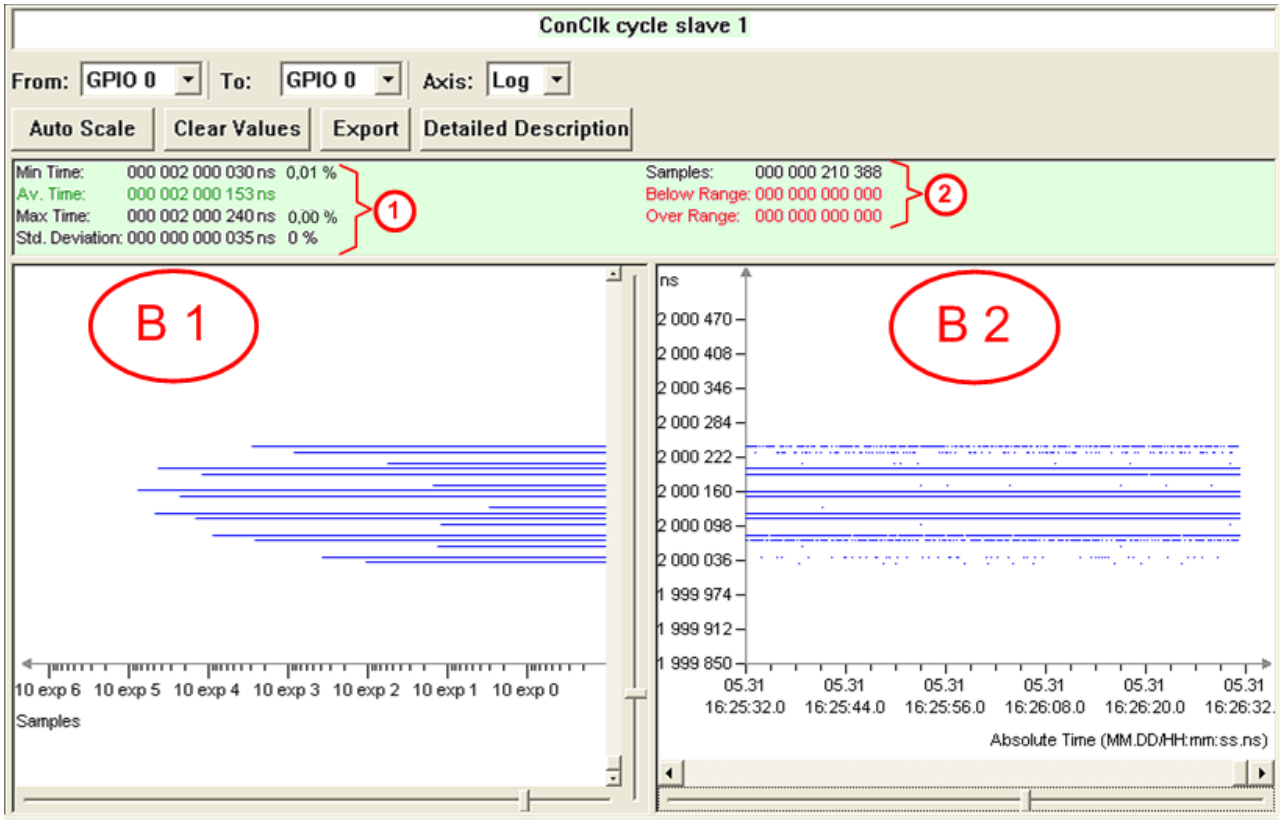


Abbildung 96: netANALYZER ConClk Zykluszeit am Slave 1

Im Fenster „**B 1**“ (dem Histogramm) sieht man die zeitliche Verteilung der einzelnen Telegramme und deren Anzahl.

© Hilscher, 2008-2012

Im Fenster „**B 2**“ (der Historie) sieht man die Verteilung der Telegramme über die Zeit.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale ConClk Zykluszeit, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	2,000 ms
Av Time	Die mittlere ConClk Zykluszeit der Telegramme..	2,000 ms
Max Time	Die maximale ConClk Zykluszeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	2,000 ms
Std. Deviation	Die Standardabweichung der ConClk Zykluszeit.	35 ns

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	210388
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

Es ist zu erkennen, dass es über die Zeit keine periodischen Veränderungen des Signals gibt.

7.2.4.3 Timing-Analyse-Fenster C: Zykluszeit des Master-Daten-Telegramms am Ausgang des Masters

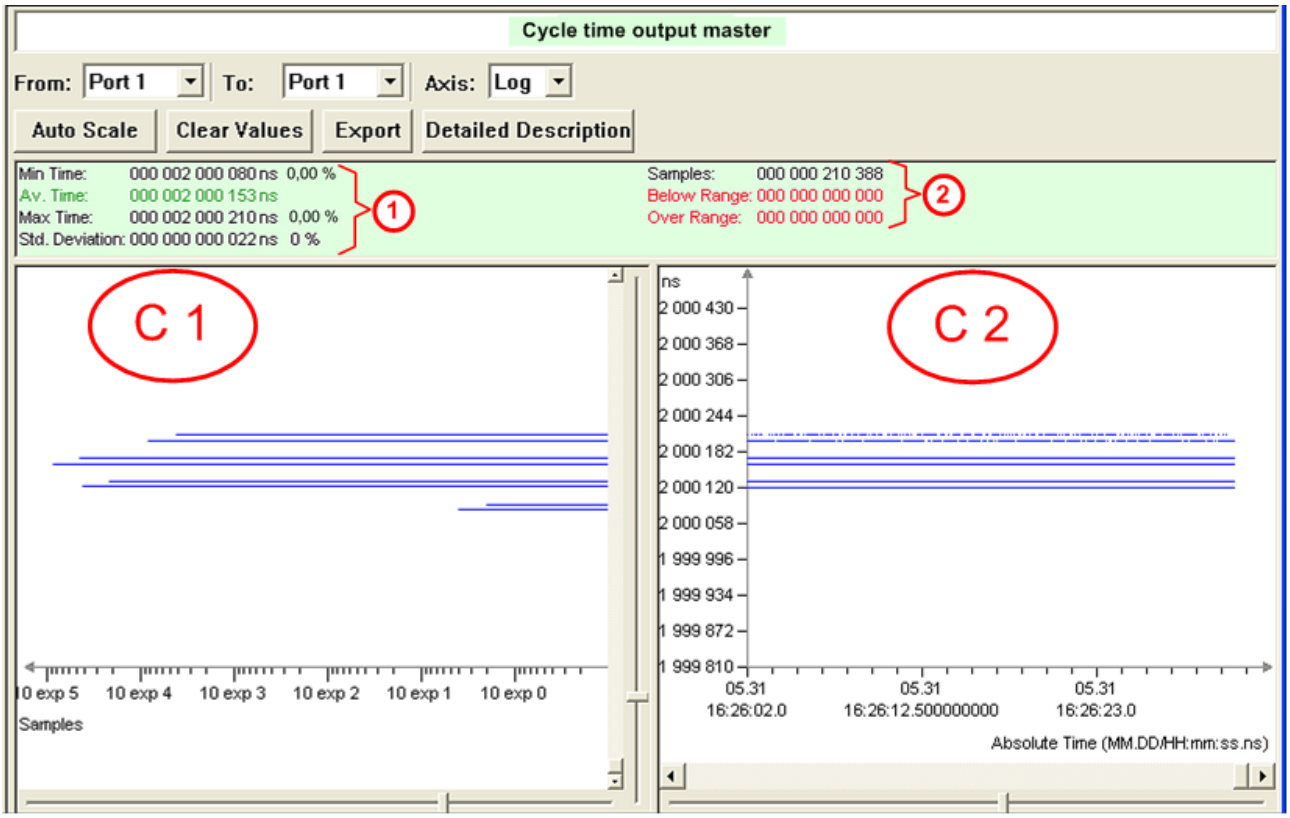


Abbildung 97: Zykluszeit Master-Daten-Telegramm Ausgang Master

Im Fenster „**C 1**“ (dem Histogramm) sieht man die zeitliche Verteilung der einzelnen Telegramme und deren Anzahl.

© Hilscher, 2008-2012

Im Fenster „**C 2**“ (der Historie) sieht man die Verteilung der Telegramme über die Zeit.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Zykluszeit des Master-Daten-Telegramms, sowie die prozentuale Abweichung zur mittleren Zykluszeit.	2,000 080 ms
Av Time	Die mittlere ConClk Zykluszeit der Telegramme..	2,000 153ms
Max Time	Die maximale ConClk Zykluszeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	2,000 210ms
Std. Deviation	Die Standardabweichung der ConClk Zykluszeit.	22 ns

Die Absolute Jitter-Zeit beträgt 130 ns.

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	210388
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

7.2.4.4 Timing-Analyse-Fenster D: Zykluszeit des Master-Daten-Telegramms nach Durchlauf von 3 Slaves

Es ist zu erwarten, dass sich der Jitter des Master-Daten-Telegramms nach dem Durchlauf durch die drei Slaves (durch deren Verarbeitung) vergrößert hat.

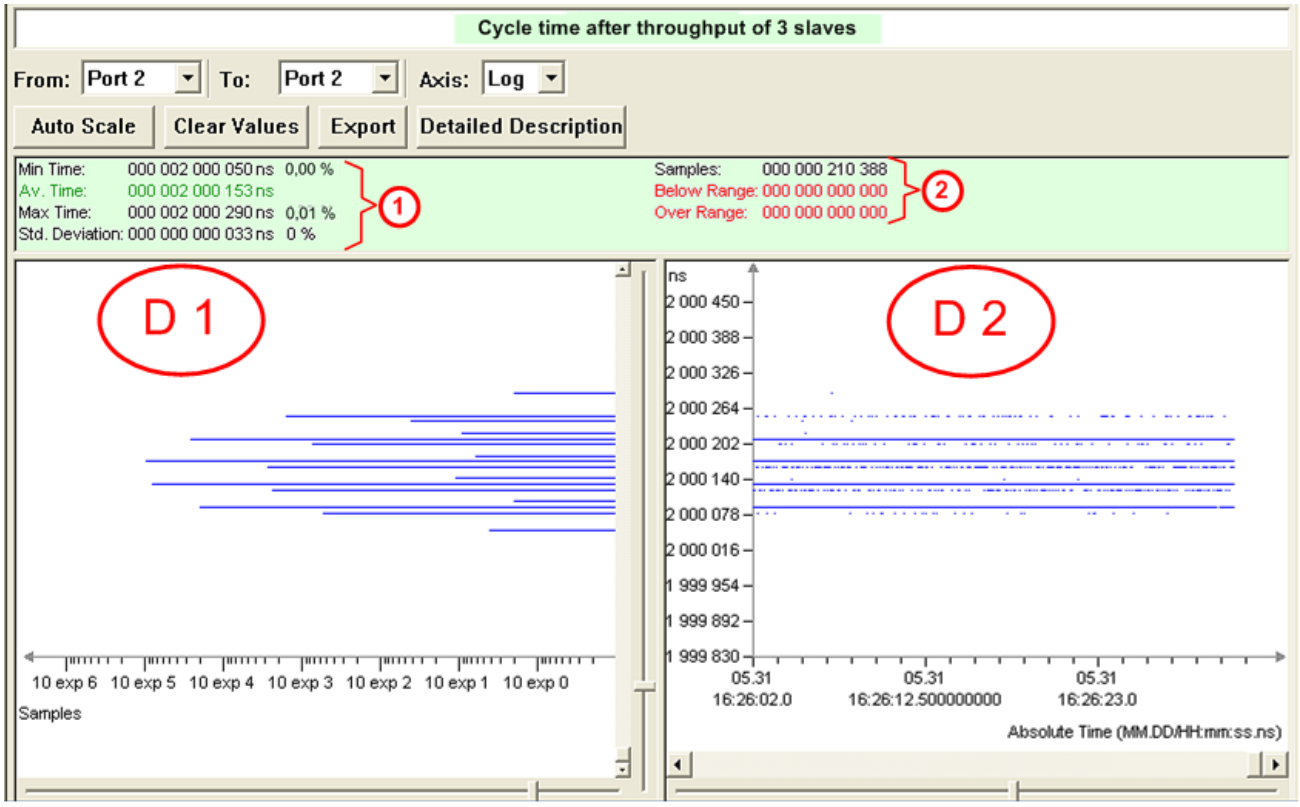


Abbildung 98: Zykluszeit Master-Daten-Telegramm nach Durchlauf von 3 Slaves

© Hilscher, 2008-2012

Im Fenster „**D 1**“ (dem Histogramm) sieht man die zeitliche Verteilung der einzelnen Telegramme und deren Anzahl.

Im Fenster „**D 2**“ (der Historie) sieht man die Verteilung der Telegramme über die Zeit.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Zykluszeit des Master-Daten-Telegramms, sowie die prozentuale Abweichung zur mittleren Zykluszeit.	2,000 050ms
Av Time	Die mittlere ConClk Zykluszeit der Telegramme..	2,000 153ms
Max Time	Die maximale ConClk Zykluszeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	2,000 290ms
Std. Deviation	Die Standardabweichung der ConClk Zykluszeit.	33 ns

Die Absolute Jitter-Zeit beträgt 230 ns und hat sich damit gegenüber dem Ausgang des Masters um 100 ns vergrößert. Ebenso ist die Standardabweichung um 11 ns größer geworden.

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	210388
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

7.3 Datenaufzeichnungen durchführen

Es sollen die Telegramme der PC-Karte cifX zu den Slaves und die Antworttelegramme von den Slaves an die PC-Karte cifX aufgezeichnet werden.

Voraussetzungen:

- Der Hardware-Aufbau, wie im Abschnitt *Hardware-Aufbau* auf Seite 87 beschrieben, muss erstellt sein,
- die Einstellungen für die PC-Karte cifX müssen erfolgt sein,
- es muss ein Datenaustausch zwischen der PC-Karte cifX und den Slaves erfolgen.

➢ Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER**.

⇘ Sie gelangen in das Hauptfenster des netANALYZERs.

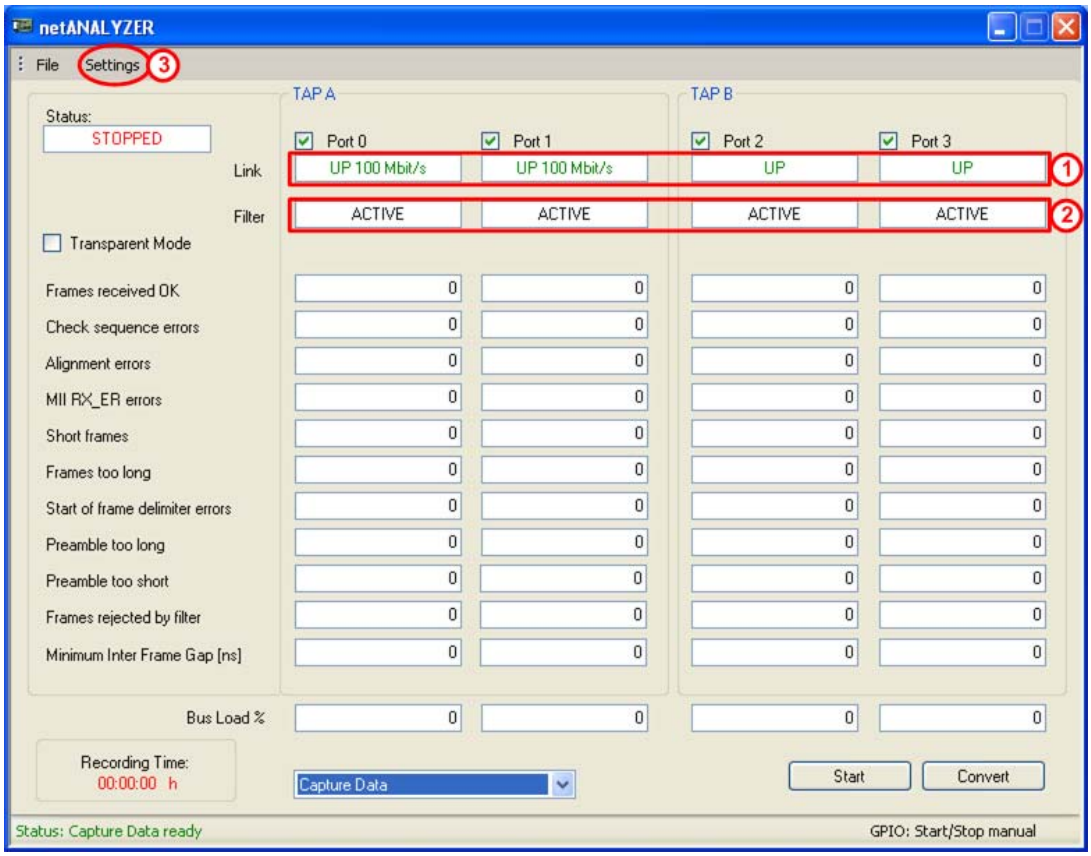


Abbildung 99: netANALYZER Hauptfenster

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 87 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP mit Baudrate** oder (bei älteren netANALYZER-Karten) nur mit **UP** gekennzeichnet.

➢ Stellen Sie sicher, dass unter dem Dialogweg (wie bei ② dargestellt) **Settings > Filter Settings**, wie bei der Zeitmessung in Abschnitt *Zeitmessung vorbereiten und durchführen* auf Seite 88 beschrieben, aktiviert sind.

⇘ Sie kommen zurück ins Hauptfenster.

© Hilscher, 2008-2012

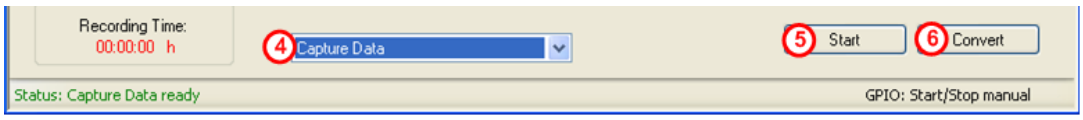


Abbildung 100: Datenaufzeichnung starten

- ➢ Stellen Sie sicher, dass **Capture Data** ④ eingestellt ist.
- ➢ Klicken Sie **Start** ⑤, um die Aufzeichnung zu starten.
- ✎ Die Schaltfläche **Start** ⑤ wird zur Schaltfläche **Stop** ⑤.
- ➢ Warten Sie bis eine ausreichende Anzahl von Telegrammen aufgezeichnet wurden.
- ➢ Klicken Sie **Stop** ⑤.
- ➢ Klicken Sie **Convert** ⑥.
- ✎ Es erscheint folgendes Fenster:

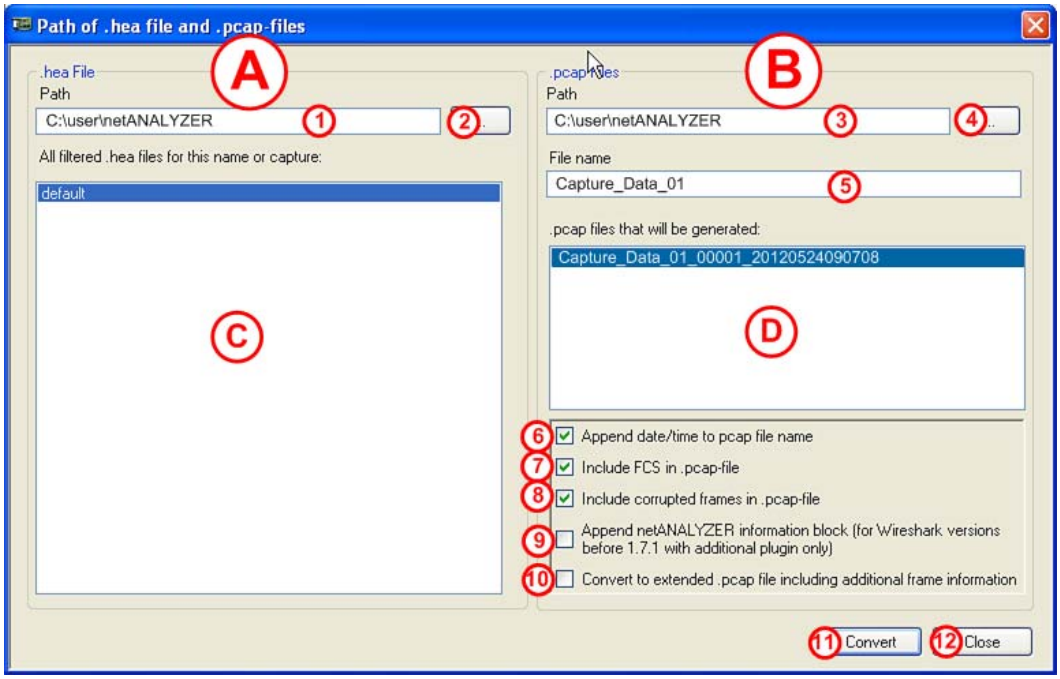


Abbildung 101: pcap-Konvertierung 1

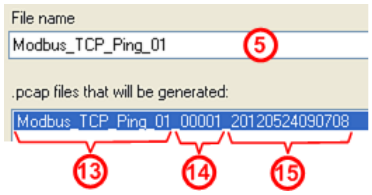
Das obige Fenster teilt sich in zwei Bereiche:

Fensterbereich Ⓐ

Bedienelement	Erläuterung
Path ①	Vom Bediener auszuwählender Pfad, aus welchem der netANALYZER die Binär-Datei (**.hea*) zur Konvertierung lesen soll. Die hier gemachten Einstellungen wirken sich auch auf die nächsten Datenaufzeichnungen aus. Die Einstellung unter **Settings > File Settings** wird damit verändert.
Schaltfläche ②	Auswahlschaltfläche zur Auswahl des Quellverzeichnisses der .hea-Dateien.
All filtered .hea files for this name or capture Ⓒ	Anzeigeliste der .hea-Dateien im ausgewähltem Verzeichnis

© Hilscher, 2008-2012

Fensterbereich (B)

Bedienelement	Erläuterung
Path (3)	Der vom Bediener zu definierende Pfad, unter welchem die **netANALYZER**-Software die konvertierte WinPcap-Datei (**.pcap*) ablegen soll.
Schaltfläche (4)	Auswahlschaltfläche zur Auswahl des Zielverzeichnis der .pcap-Dateien.
File name (5)	Systematische Dateibezeichnung für die **.pcap*-Dateien. Die **netANALYZER**-Software vergibt zusätzlich für jede Datei noch eine fortlaufende Nummer im Dateinamen.
.pcap files that will be generated (D)	Vorschau der zu erzeugenden **.pcap*-Dateien. Dabei ist der Namensaufbau wie folgt:  (13) der unter (5) ausgewählte Dateiname. (14) laufende Zählnummer (15) Zeitinformation, bestehend aus: yyyymmddhhmmss (Beginn der Aufzeichnung der hea-Datei, (nur wenn (6) der Haken gesetzt wurde.).
Append date/time to pcap file name (6)	Ist der Haken gesetzt, werden Datum und Zeit im Dateinamen ergänzt.
Include FCS in .pcap-files (7)	Checkbox ob die Ethernet-Prüfsumme mit in der PCAP-Datei enthalten sein soll oder nicht. (Einige Wireshark-Dissectoren unterstützen FCS nicht.) **Hinweis:** Wenn **Convert to extended .pcap file including additional frame information** angehakt ist, ist **Include FCS in .pcap-file** ausgegraut, da FCS dann immer in eine .pcap-Datei konvertiert wird. FCS = Frame Check Sequence (Ethernet-Prüfsumme) Nicht auswählbar, wenn Option (10) angehakt, jedoch aktiv.
Include corrupted frames in .pcap file (8)	Ist diese Option aktiviert, werden auch fehlerhafte Frames in die .pcap-Datei übernommen. Ist die Option deaktiviert werden nur korrekte Telegramme in der .pcap-Datei gespeichert.
Append netANALYZER information block (for Wireshark versions before 1.7.1 with additional plug in only) (9)	Die Option erfordert für Wireshark-Versionen < V1.7.1 die Installation des netANALYZER-Wireshark-Plugins. Fügt den netANALYZER-Info-Block nach dem Ethernet-Frame in die .pcap-Dateien ein. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen. **Hinweis:** Das .pcap-Dateiformat mit dem Info-Block nach dem Ethernet-Frame wird von Wireshark-Versionen ≥ 1.7.1 nicht mehr unterstützt. Nicht auswählbar, wenn Option (10) angehakt.
Convert to extended .pcap file including additional frame information (10)	**Hinweis:** Wird dieser Haken gesetzt, kann das mit der netANALYZER-Software V1.4.x.x erzeugte erweiterte .pcap-Dateiformat nur in Wireshark-Versionen ab V1.7.1 geöffnet werden. Ab der Version der netANALYZER-Software V1.4.x.x kann ein erweitertes .pcap-Dateiformat erzeugt werden. Dabei befindet sich der „netANALYZER Info-Block“ in den 4 Bytes vor dem Ethernet-Frame. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen.
Convert (11)	Die Konvertierung der Binär-Dateien ins WinPcap-Format wird gestartet.
Close (12)	Sie schließen das Fenster ohne eine Konvertierung zu starten.

- Wählen Sie im Fensterbereich (A) die zu konvertierende Datei aus.
- Ergänzen Sie die notwendigen Einstellungen im Fensterbereich (B).
- Klicken Sie auf die Schaltfläche **Convert** (11), um die Daten ins pcap-Format zu konvertieren.

Nach Abschluss des Konvertierungsvorgangs schließt sich das Fenster.

© Hilscher, 2008-2012

➢ Öffnen Sie die Datei mit Wireshark.
Wenn das Programm Wireshark korrekt installiert ist, wird mittels eines Doppelklicks auf die .pcap-Datei diese mit Wireshark geöffnet.

Es werden folgende Daten angezeigt:

Das Programm Wireshark zeigt die Daten wie folgt an:

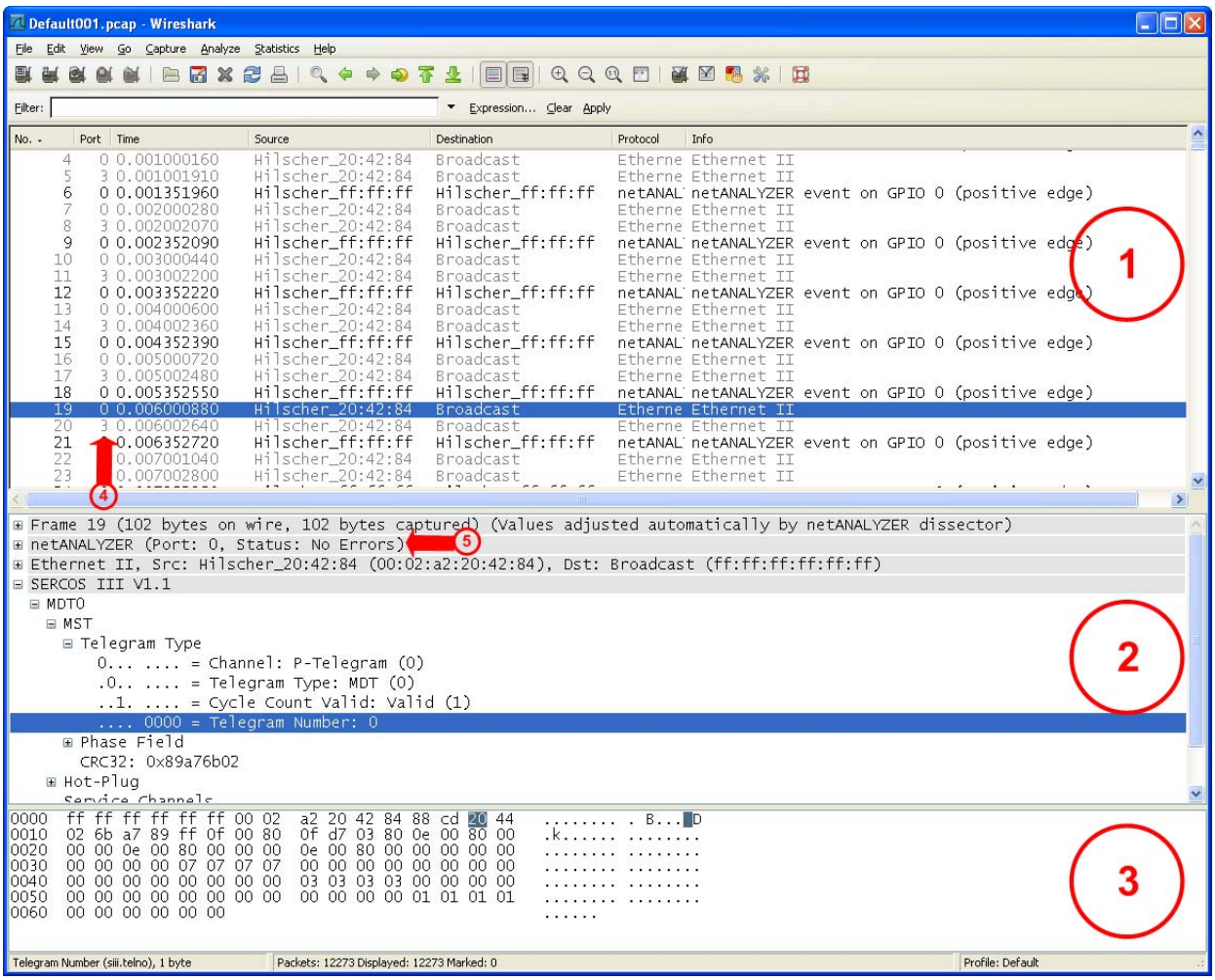

Default001.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Port Time Source Destination Protocol Info
4 0 0.001000160 Hilscher_20:42:84 Broadcast Etherne Ethernet II
5 3 0.001001910 Hilscher_20:42:84 Broadcast Etherne Ethernet II
6 0 0.001351960 Hilscher_ff:ff:ff Hilscher_ff:ff:ff netANAL netANALYZER event on GPIO 0 (positive edge)
7 0 0.002000280 Hilscher_20:42:84 Broadcast Etherne Ethernet II
8 3 0.002002070 Hilscher_20:42:84 Broadcast Etherne Ethernet II
9 0 0.002352090 Hilscher_ff:ff:ff Hilscher_ff:ff:ff netANAL netANALYZER event on GPIO 0 (positive edge)
10 0 0.003000440 Hilscher_20:42:84 Broadcast Etherne Ethernet II
11 3 0.003002200 Hilscher_20:42:84 Broadcast Etherne Ethernet II
12 0 0.003352220 Hilscher_ff:ff:ff Hilscher_ff:ff:ff netANAL netANALYZER event on GPIO 0 (positive edge)
13 0 0.004000600 Hilscher_20:42:84 Broadcast Etherne Ethernet II
14 3 0.004002360 Hilscher_20:42:84 Broadcast Etherne Ethernet II
15 0 0.004352390 Hilscher_ff:ff:ff Hilscher_ff:ff:ff netANAL netANALYZER event on GPIO 0 (positive edge)
16 0 0.005000720 Hilscher_20:42:84 Broadcast Etherne Ethernet II
17 3 0.005002480 Hilscher_20:42:84 Broadcast Etherne Ethernet II
18 0 0.005352550 Hilscher_ff:ff:ff Hilscher_ff:ff:ff netANAL netANALYZER event on GPIO 0 (positive edge)
19 0 0.006000880 Hilscher_20:42:84 Broadcast Etherne Ethernet II
20 3 0.006002640 Hilscher_20:42:84 Broadcast Etherne Ethernet II
21 0.006352720 Hilscher_ff:ff:ff Hilscher_ff:ff:ff netANAL netANALYZER event on GPIO 0 (positive edge)
22 0.007001040 Hilscher_20:42:84 Broadcast Etherne Ethernet II
23 0.007002800 Hilscher_20:42:84 Broadcast Etherne Ethernet II
1
4
Frame 19 (102 bytes on wire, 102 bytes captured) (Values adjusted automatically by netANALYZER dissector)
netANALYZER (Port: 0, Status: No Errors)
5
Ethernet II, Src: Hilscher_20:42:84 (00:02:a2:20:42:84), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
SERCOS III V1.1
MDT0
MST
Telegram Type
0... .... = Channel: P-Telegram (0)
.0.. .... = Telegram Type: MDT (0)
..1. .... = Cycle Count Valid: Valid (1)
.... 0000 = Telegram Number: 0
Phase Field
CRC32: 0x89a76b02
Hot-Plug
Service Channels
2
0000 ff ff ff ff ff ff 00 02 a2 20 42 84 88 cd 20 44 ..... . B... D
0010 02 6b a7 89 ff 0f 00 80 0f d7 03 80 0e 00 80 00 .k..... .....
0020 00 00 0e 00 80 00 00 00 0e 00 80 00 00 00 00 00 ....
0030 00 00 00 00 07 07 07 07 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 00 00 03 03 03 03 00 00 00 00 ....
0050 00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 01 ....
0060 00 00 00 00 00 00 ......
3
Telegram Number (siii.telno), 1 byte
Packets: 12273 Displayed: 12273 Marked: 0
Profile: Default

Abbildung 102: SERCOS III Wireshark Telegrammdarstellung

① In diesem Fensterbereich sehen Sie die Auflistung aller entsprechend der Filtereinstellung detektierten Telegramme. Bei ④ sehen Sie hier an welchem Port der netANALYZER-Karte das Telegramm angekommen ist.

Hinweis: Sollte im Fensterbereich ① der Text **Event on GPIO…** fehlen, so ist der Hilscher Wireshark-Dissector nicht aktiviert. Führen Sie die Aktivierung entsprechend des *Benutzerhandbuch netANALYZER Rev. 12,* Abschnitt 14.4 durch.

② In diesem Fensterbereich können Sie einzelne Telegrammbereiche des ausgewählten Telegramms betrachten. Bei ⑤ sehen Sie hier an welchem Port der netANALYZER-Karte das Telegramm angekommen ist.

Achtung! Um die oben dargestellte auskommentierte Darstellung (im Fensterbereich ②) zu bekommen, müssen Sie sich ggf. noch ein Plugin von der SERCOS Homepage „https://www.sercos.org“ für das Wireshark-Programm herunterladen.

③ In diesem Fensterbereich werden die Daten des ausgewählten Telegramms auf Byteebene dargestellt.

© Hilscher, 2008-2012

8 Modbus/TCP Analyse

Beispielhaft werden hier folgende Messungen durchgeführt:

- Messung der Reaktionszeit vom Slave 3,
- Messung der Durchlaufzeit der Telegramme für Slave 3 durch Slave 1 und 2,
- Messung der Zykluszeit der cifX-Telegramme,
- Messung der Netzlast mit Modbus/TCP-Telegrammen beim Netzwerkanlauf und Ping.

8.1 Hardware-Aufbau

Für diese Beispielmessung wird folgender Hardware-Aufbau benötigt.

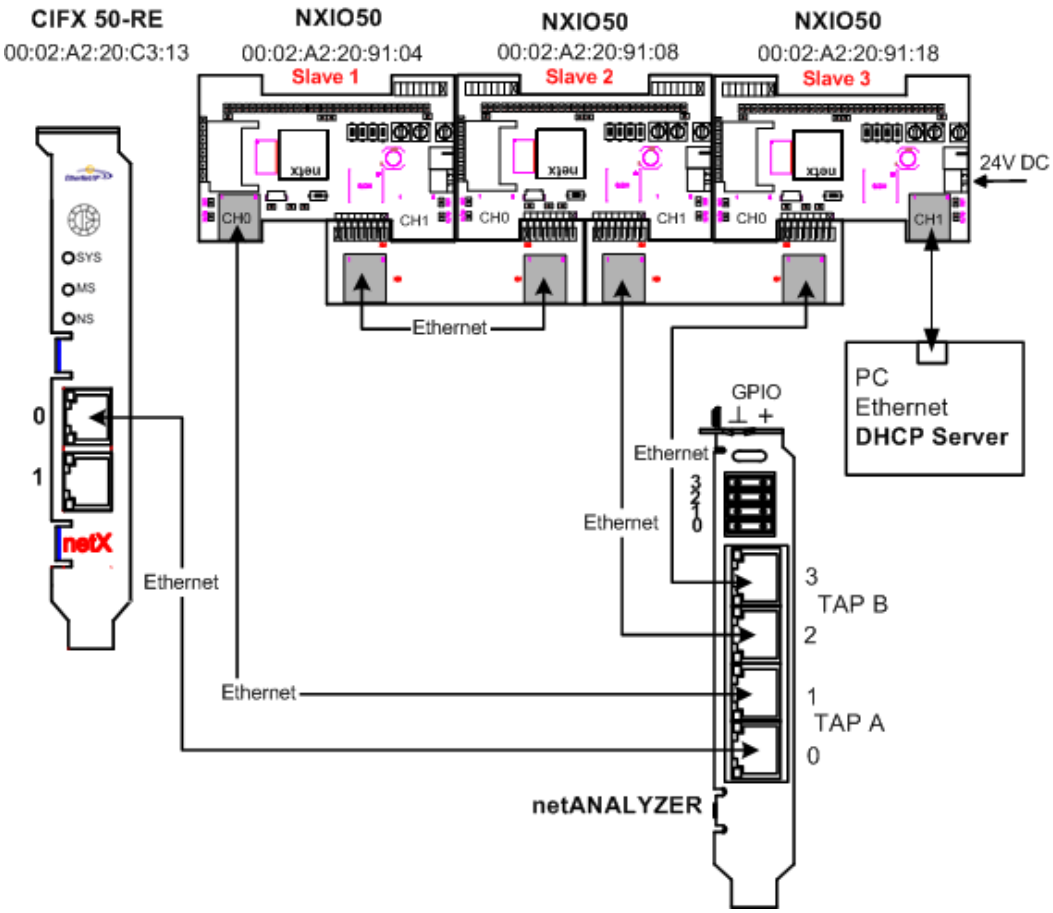


Abbildung 103: Modbus/TCP Hardware-Aufbau

Die für den in diesem Aufbau geltenden MAC-Adressen sind oberhalb der Komponenten angegeben.

Beachten Sie bitte, dass die jeweilige MAC-Adresse auf der Welt einmalig ist. Daher haben die Geräte in Ihrem Messaufbau andere MAC-Adressen.

Hinweis: Die Einstellungen für die NXIO 50 Boards müssen entsprechend Abschnitt 6.6 des *Benutzerhandbuch Real-Time-Ethernet-Kit - Kommunikationssysteme für Real-Time-Ethernet Installation, Bedienung und Konfiguration* vorgenommen worden sein..

© Hilscher, 2008-2012

Hinweis: Achten Sie darauf, dass Sie während der Messung mit dem PC nicht am Hausnetz angeschlossen sind, mindestens jedoch vom Hausnetz mittels eines Switch entkoppelt sind, da es sonst Fehlmessungen gibt.

8.2 Zeitmessung vorbereiten und durchführen

Hinweis: Die NXIO-Boards verfügen über eine Autocrossover-Funktionalität. Daher ist ein vertauschen der Kabel am netANALYZER am TAP A (Port 0 und Port 1) sowie am TAP B (Port 2 und Port 3) ohne Bedeutung. Somit sind auch bei der Anzeige der Analysewerte die Portbezeichnungen 0/1 bzw. 2/3 als vertauschbar zu betrachten.

Hinweis: Hier sind nur die für diesen Messaufbau unmittelbar erforderlichen Einstellungen des netANALYZERs beschrieben. Detaillierte Informationen über die Einstell- und Aufzeichnungsmöglichkeiten der Software entnehmen Sie bitte der Dokumentation *Benutzerhandbuch netANALYZER.*

8.2.1 Zeitmessung vorbereiten

- Starten Sie die netANALYZER Software mit **Start >Programme > Hilscher GmbH > Hilscher netANALYZER**.

Sie gelangen ins Hauptfenster des netANALYZERs.

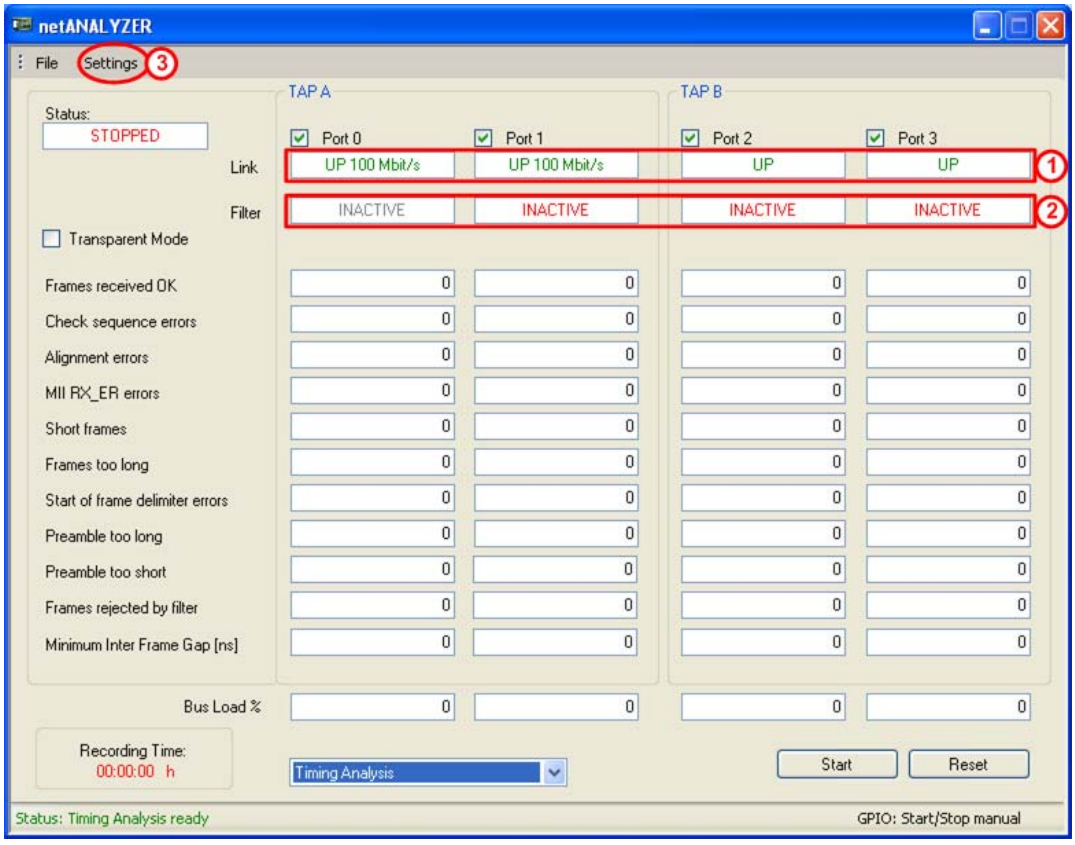


Abbildung 104: Modbus/TCP netANALYZER Start

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 102 beschrieben) aufgebaut haben und die Kommunikation zwischen dem PC und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie

© Hilscher, 2008-2012

bei (1) dargestellt) als **UP** bzw. UP mit Baudrate (hier UP 100 Mbit/s) gekennzeichnet. Unter (2) können Sie sehen, ob ein Filter eingestellt ist (ACTIVE). Ist dieses der Fall, kontrollieren Sie, ob die Filtereinstellungen für den aktuellen Messaufbau korrekt sind.

Wegen der Autocrossover-Funktionalität der Ports ist zunächst festzustellen, über welche Ports die Kommunikation cifX nach Slave 3 läuft. Hierzu sind bestimmte Filtereinstellungen erforderlich.

➢ Öffnen Sie im Hauptfenster des Programms **Settings > Filter Settings** (3) die Filtereinstellungen.

↬ Das Filter-Fenster erscheint wie folgt.

8.2.2 Filter einstellen

1. Es ist zunächst festzustellen über welche Ports die Kommunikation in welche Richtung stattfindet. Deshalb wird zuerst ein Filter für die Telegramme von der cifX zum Slave 3 definiert.

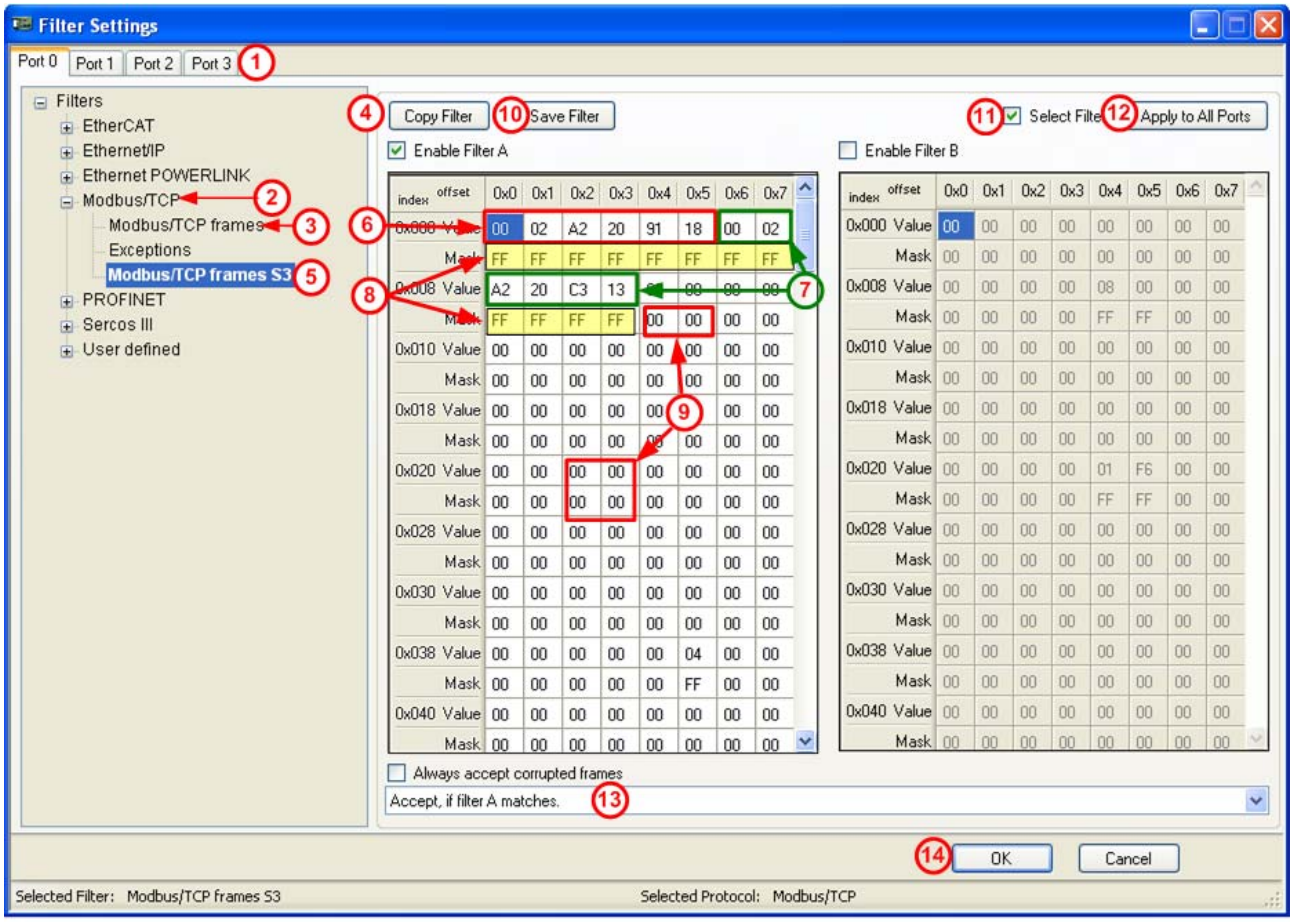


Abbildung 105: Modbus/TCP netANALYZER Filter 1

➢ Nehmen Sie folgende Filtereinstellungen (entsprechend obiger Abbildung) vor:

➢ Wählen Sie einen Port (1) für den Sie die Einstellungen machen möchten. Zunächst ist diese Auswahl unbedeutend, da im ersten Schritt das Filter für alle Ports identisch eingestellt wird.

➢ Wählen Sie **Filters > Modbus/TCP** (2) **> Modbus/TCP frames** (3) aus.

➢ Kopieren Sie diesen Filter mit **Copy Filter** (4).

© Hilscher, 2008-2012

- Vergeben Sie für den kopierten Filter einen Namen (hier **Modbus/TCP frames S3** (5)).
- Tragen Sie in den rot markierten Bereich (6) die MAC-Zieladresse der Telegramme ein. Hier ist es die MAC-Adresse vom Slave 3.
- Tragen Sie in den grün markierten Bereich (7) die MAC-Quelladresse der Telegramme ein. Hier ist es die Mac-Adresse der PC-Karte cifX.
- Tragen Sie in die Maske „**FF**“ (8) ein, damit auf exakt den vorgegebenen Werten verglichen wird.
- Überschreiben Sie die in den beiden markierten Bereichen bestehenden Einträge mit „**00**“ (9).
- Sichern Sie die Filtereinstellungen mit **Save Filter** (10).
- Wählen Sie den soeben erstellten Filter für den angewählten Port aus, d. h. setzen Sie den Haken bei **Select Filter** (11).
- Kontrollieren Sie, ob in der Auswahl **Accept, if filter A matches** (12) ausgewählt ist. (Diese Auswahl ist nur möglich, wenn kein Haken bei **Enable Filter B** gesetzt ist.)
- Klicken Sie **Apply to All Ports** (13), damit die Filtereinstellungen für alle Ports wirksam wird.
- Verlassen Sie die Filtereinstellungen mit **OK** (14).
- Sie gelangen zurück ins Hauptfenster des netANALYZERs.

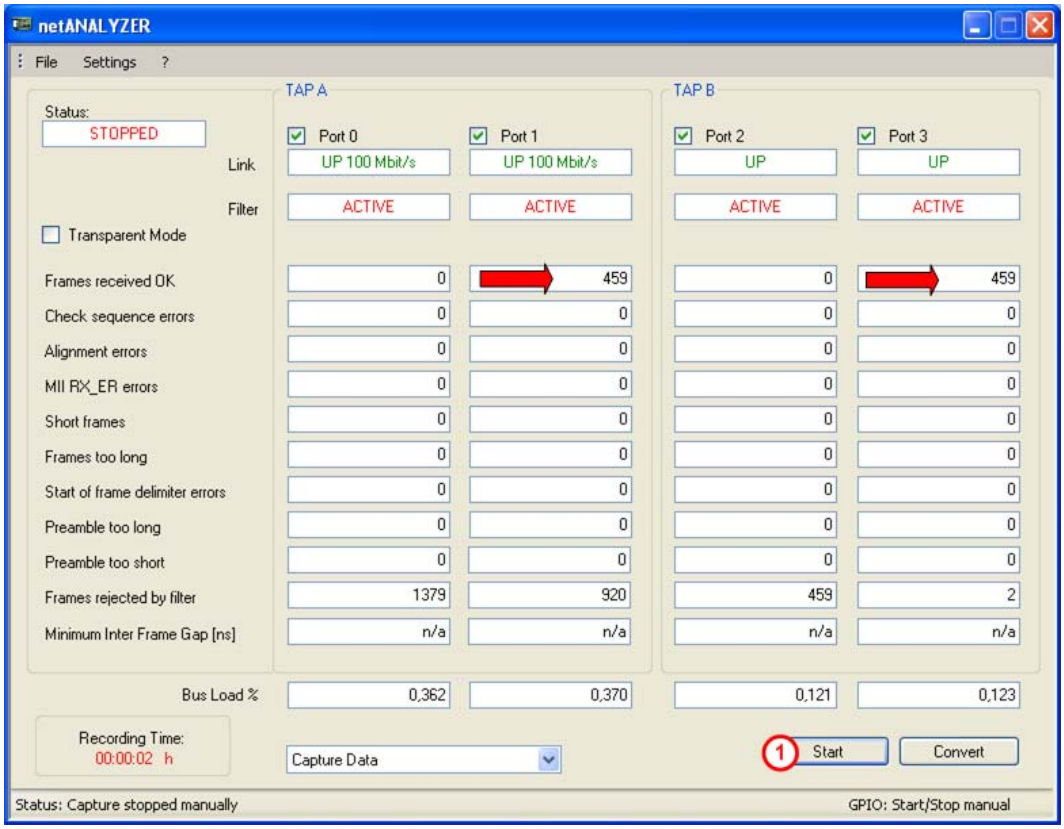


Abbildung 106: Modbus/TCP netANALYZER Filter 1 Test

- Starten Sie kurzzeitig die Timing-Analyse mit **Start** (1) und anschließend **Stop** (dieselbe Schaltfläche).
- Nun können Sie in der obigen Abbildung sehen, dass in der Spalte **Frames received OK** unter Port 1 und Port 3 Telegramme gezählt wur-

© Hilscher, 2008-2012

den. Daraus ist zu entnehmen, dass die Telegramme von der cifX (Client) zum Slave 3 über Port 1 und Port 3 laufen.

Hinweis: Wegen der Autocrossover-Funktionalität. der Ports der netANALYZER-Karte können bei Ihrem Testaufbau. die Telegramme auch über Port 1 und Port 2 laufen. Passen Sie dann die folgenden Einstellungen entsprechend an.

2. Nun ist ein Filter für die Antwort von Slave 3 an die PC-Karte cifX zu erstellen.

- Öffnen Sie mit **Settings > Filter Settings** (3) erneut die Filtereinstellungen.
- Kopieren Sie den von Ihnen angelegten Filter, um einen Filter für den Signalweg vom Slave 3 zum Client (PC-Karte cifX) zu erstellen.
  Gehen Sie dabei wie folgt vor:

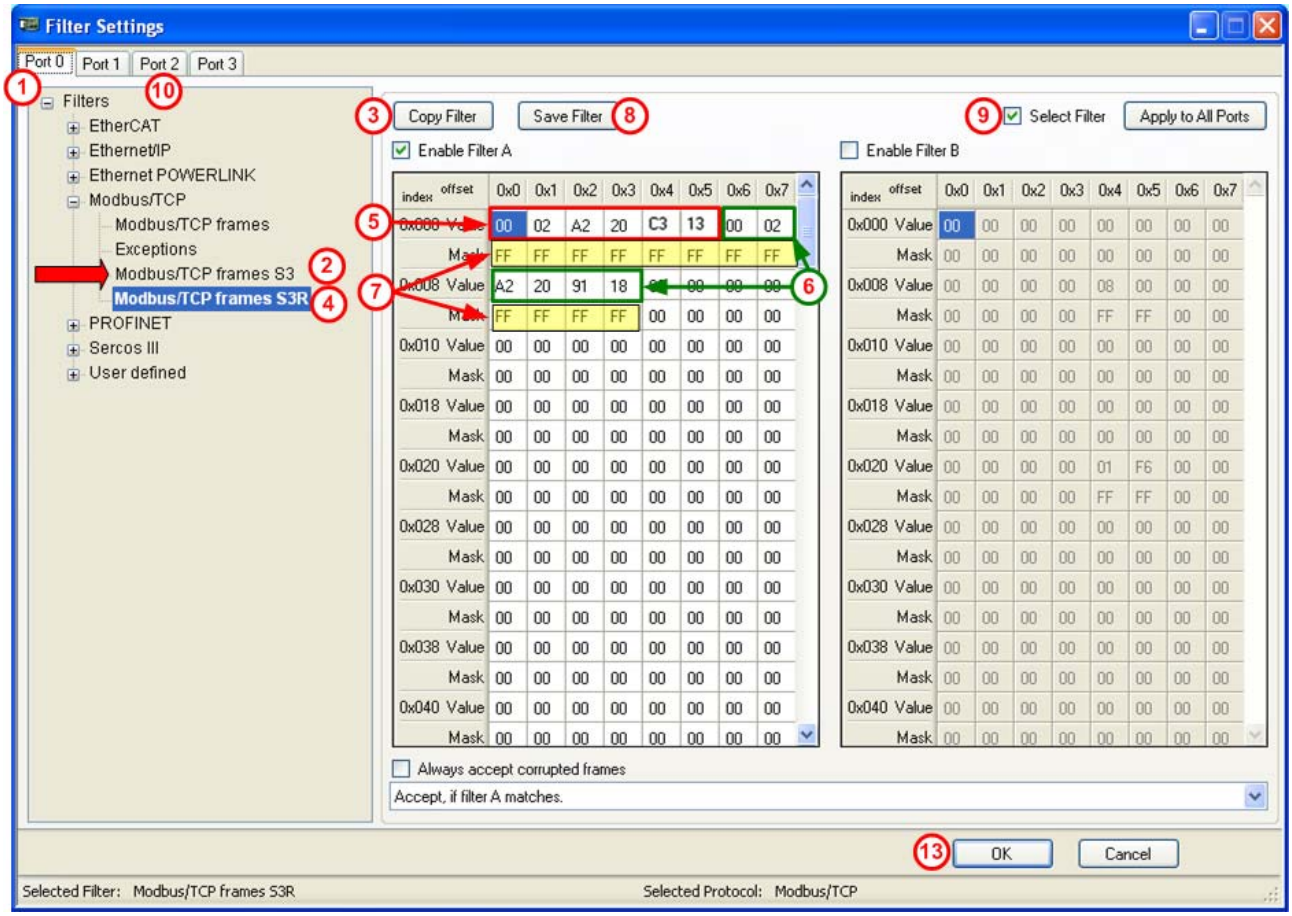


Abbildung 107: Modbus/TCP netANALYZER Filter 2

- Wählen Sie einen Port aus, der in der vorhergehenden Signalaufzeichnung keine Telegramme detektiert hatte. Hier ist es Port 0 (1).
- Wählen Sie den zuvor angelegten Filter **Modbus/TCP frames S3** (2).
- Klicken Sie **Copy Filter** (3), um den Filter zu kopieren.
- Vergeben Sie einen neuen Namen für den kopierten Filter, hier **Modbus/TCP frames S3R** (4).
- Tragen Sie im markierten Bereich (5) die MAC-Zieladresse der Telegramme vom Slave 3 ein. Hier ist es die MAC-Adresse der cifX.

© Hilscher, 2008-2012

- Tragen Sie im markierten Bereich ⑥ die MAC-Quelladresse des Slaves 3 ein.
- Tragen Sie in die Maske „**FF**“ ⑦ ein, damit auf exakt den vorgegebenen Werten verglichen wird.
- Speichern Sie die Filtereinstellungen mit **Save Filter** ⑧.
- Wählen Sie diesen Filter für diesen Port (hier Port 0) ⑨ aus. (An Tap A der netANALYZER-Karte den Port der beim ersten Test keine Telegramme selektiert hat.)
- Wählen Sie für Tap B den Port ⑩ aus, der keine Telegramme selektiert hatte (Hier ist es Port 2). Klicken Sie den neu angelegten Filter ④ an, um ihn auszuwählen.
- Klicken Sie **Select Filter** ⑨, um den Filter für diesen Port zu aktivieren.
- Wechseln Sie in den Filter **Modbus/TCP frames S3.**

Hier selektieren Sie auf die Telegramme mit dem Funktionscode FC 4.

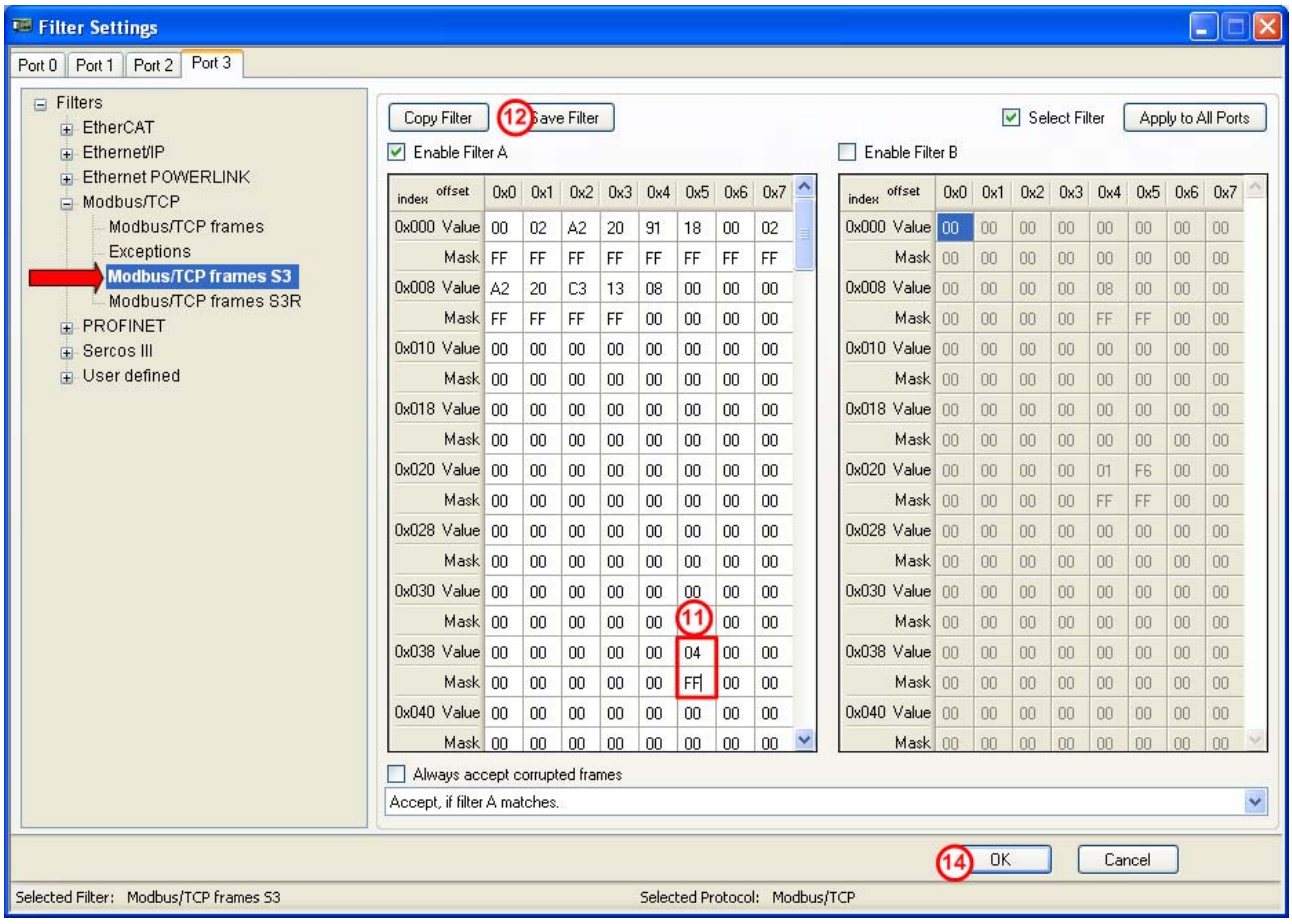


Abbildung 108: Modbus/TCP netANALYZER Filter 3

Gehen Sie wie folgt vor:

- Tragen Sie an der Filterposition ⑪ (Zeile 0x038, Spalte 0x5) **04** für den Funktionscode FC 4 ein. In der Zeile darunter dann den Maskeneintrag „**FF**“.
- Speichern Sie die Änderung mit **Save Filter** ⑫.
- Verlassen Sie den Filter-Dialog mit **OK** ⑬.
- Sie gelangen zurück in das Hauptfenster des netANALYZERs.

© Hilscher, 2008-2012

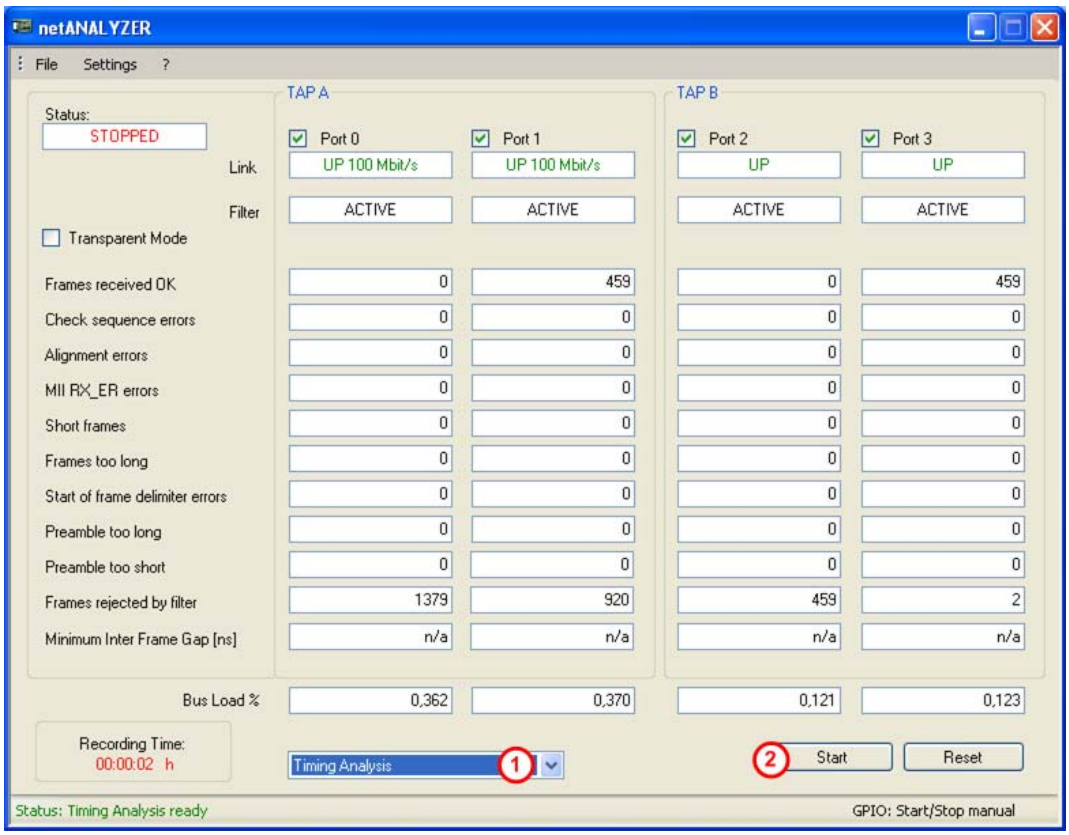


Abbildung 109: Modbus/TCP netANALYZER Start Timing Analyse

- Wählen Sie **Timing Analysis** (1).

  Es öffnet sich im Vordergrund das Fenster zur grafischen Darstellung der Zeitanalyse (Timing Analysis).

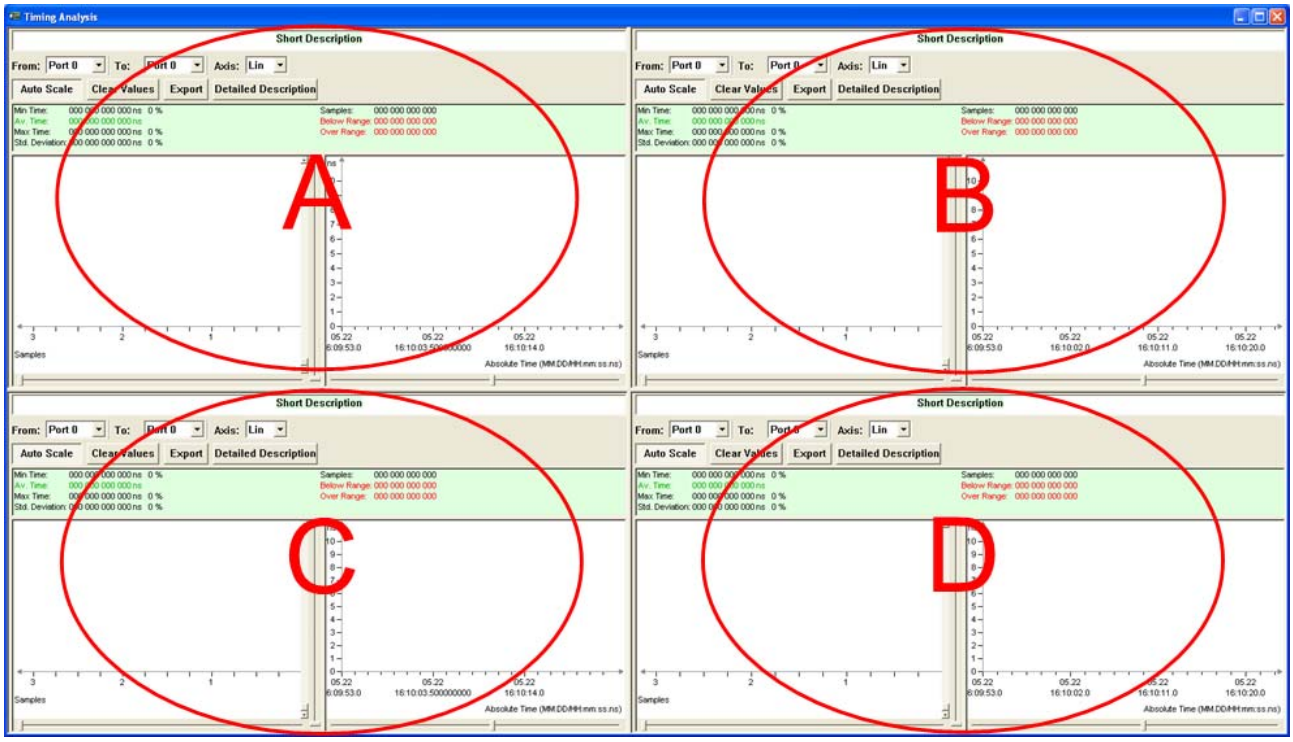


Abbildung 110: netANALYZER Timing-Analyse-Fenster

Das Timing Analysis-Fenster unterteilt sich in 4 Unterfenster, die wiederum 2 Teilfenster (Histogramm und Historie) beinhalten. Im weiteren Verlauf die-

© Hilscher, 2008-2012

ses Messaufbaus wird in der Regel immer nur ein Unterfenster angesprochen.

Die Größe der Einzelfenster können Sie durch ziehen des Kreuzungspunktes der Fensterteilungslinien verändern.

Sie können sich auch nur das Historie- oder Histogramm-Fenster anzeigen lassen. Dieses können Sie im Haupt-Fenster des netANALYZERs unter **Settings > Analysis Configuration** einstellen.

8.2.3 Einstellungen in den Timing-Analysefenstern

Achten Sie darauf, dass in allen Unterfenstern zunächst **Auto Scale** (1) eingestellt ist.

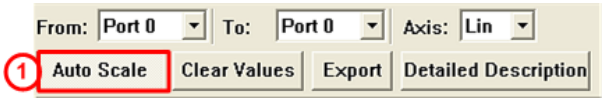


Abbildung 111: netANALYZER Timing-Auto-Scale

Damit stellen Sie sicher, dass (wenn Telegramme detektiert werden) diese auch als Balken sichtbar sind und nicht außerhalb des Zeitstrahls liegen. (Achtung: Der Zeitstrahl geht in dieser Darstellung senkrecht nach oben.)

- Stellen Sie die From / To - Bedingungen für jedes Teilfenster wie folgt ein:

Hinweis: Wegen der Autocrossover-Funktionalität. der Ports der netANALYZER-Karte können bei Ihrem Testaufbau. die Telegramme ggf. auch über die entsprechenden korrespondierenden Port laufen. Passen Sie die Ports entsprechend Ihres Aufbaus an.

8.2.3.1 Einstellungen für Analysefenster A: Telegrammdurchlaufzeit

Hier soll die Telegrammdurchlaufzeit (der Telegramme von der cifX zum Slave 3) durch Slave 1 und 2 ermittelt werden.

Abbildung 112: Modbus/TCP netANALYZER Messfenstereinstellungen 1

In der Kopfzeile können Sie einen beschreibenden Text für die Messung eingeben (1).

Startport **From**: der Messung (hier Port 1 (2)), der Port an dem die Telegramme von der PC-Karte cifX aus vor dem ersten Slave erfasst werden.

Zielport **To**: der Messung (hier Port 3 (3)), der Port an dem die Telegramme nach dem Durchlauf von Slave 1 und 2 an der netANALYZER-Karte ankommen.

Achten Sie darauf, dass **Auto Scale** (5) eingeschaltet ist, damit die Messergebnisse immer im Anzeigefenster sichtbar sind.

© Hilscher, 2008-2012

8.2.3.2 Einstellungen für Analysefenster B: Antwortzeit

Hier soll die Antwortzeit von Slave 3 gemessen werden.

Abbildung 113: Modbus/TCP netANALYZER Messfenstereinstellungen 2

In der Kopfzeile können Sie einen beschreibenden Text für die Messung eingeben (1).

Startport **From** der Messung (hier Port 3 (2)), der Port an dem die Telegramme den Slave 3 erreichen.

Zielport **To**: der Messung (hier Port 2 (3)), der Port an dem die Antwort-Telegramme vom Slave 3 ankommen.

Achten Sie darauf, dass **Auto Scale** (5) eingeschaltet ist, damit die Messergebnisse immer im Anzeigefenster sichtbar sind.

8.2.3.3 Einstellungen für Analysefenster C: Durchlaufzeit

Hier wollen wir die Telegrammdurchlaufzeit (der Telegramme vom Slave 3 an die cifX) durch Slave 1 und 2 ermitteln.

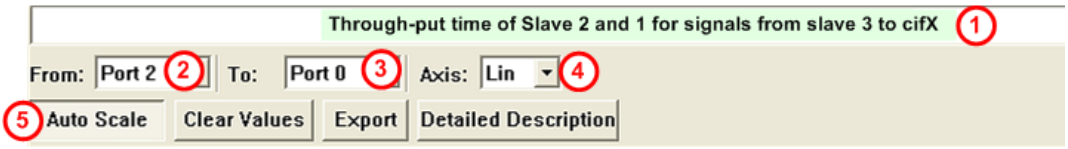


Abbildung 114: Modbus/TCP netANALYZER Messfenstereinstellungen 3

In der Kopfzeile können Sie einen beschreibenden Text für die Messung eingeben (1).

Startport **From** der Messung (hier Port 2) (2), der Port an dem die Antwort-Telegramme vom Slave 3 ankommen.

Zielport **To**: der Messung (hier Port 0) (3), der Port an dem die Antwort-Telegramme vom Slave 3 nach durchlauf durch Slave 2 und Slave 1 ankommen (3).

Achten Sie darauf, dass **Auto Scale** (5) eingeschaltet ist, damit die Messergebnisse immer im Anzeigefenster sichtbar sind.

8.2.3.4 Einstellungen für Analysefenster D: Zykluszeit

Hier soll die Zykluszeit der Telegramme von der cifX zu messen.

Abbildung 115: Modbus/TCP netANALYZER Messfenstereinstellungen 4

In der Kopfzeile können Sie einen beschreibenden Text für die Messung eingeben (1).

Startport **From** der Messung (hier Port 1 (2)), der Port an dem die Telegramme von der PC-Karte cifX ankommen.

© Hilscher, 2008-2012

Zielport **To**: der Messung (hier Port 1) ③. Der Start- und Stopp-Port ist hier identisch, um die Zykluszeit der Telegramme messen zu können ③.

Achten Sie darauf, dass **Auto Scale** ⑤ eingeschaltet ist, damit die Messergebnisse immer im Anzeigefenster sichtbar sind.

8.2.4 Messungen durchführen

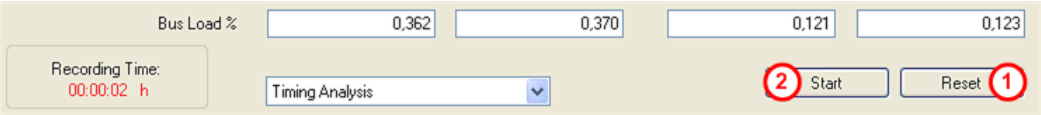


Abbildung 116: Modbus/TCP netANALYZER Start / Stopp Analyse

- ➢ Klicken Sie im Hauptfenster des netANALYZERs **Reset** ①. Damit werden die bisher aufgezeichneten Zeitdaten gelöscht.
- ➢ Klicken Sie **Start** ② um die Analyse zu starten.
- ↬ Die Schaltfläche **Start** wird zur Schaltfläche **Stop**.
- ➢ Warten Sie die Zeit, in der Sie Telegramme auswerten möchten.

Hinweis: Wollen Sie während der laufenden Analyse sich einzelne Teilbereiche ansehen, schalten Sie für das Fenster **Auto Scale** aus.

- ➢ Klicken Sie **Stop**.
- ↬ In den Fenstern finden Sie jetzt folgende Informationen:

© Hilscher, 2008-2012

8.2.4.1 Im Fenster A: Telegrammdurchlaufzeit

Die Durchlaufzeit der FC4 Telegramme die von der PC-Karte cifX an den Slave (Server) 3 durch Slave 1 und Slave 2.

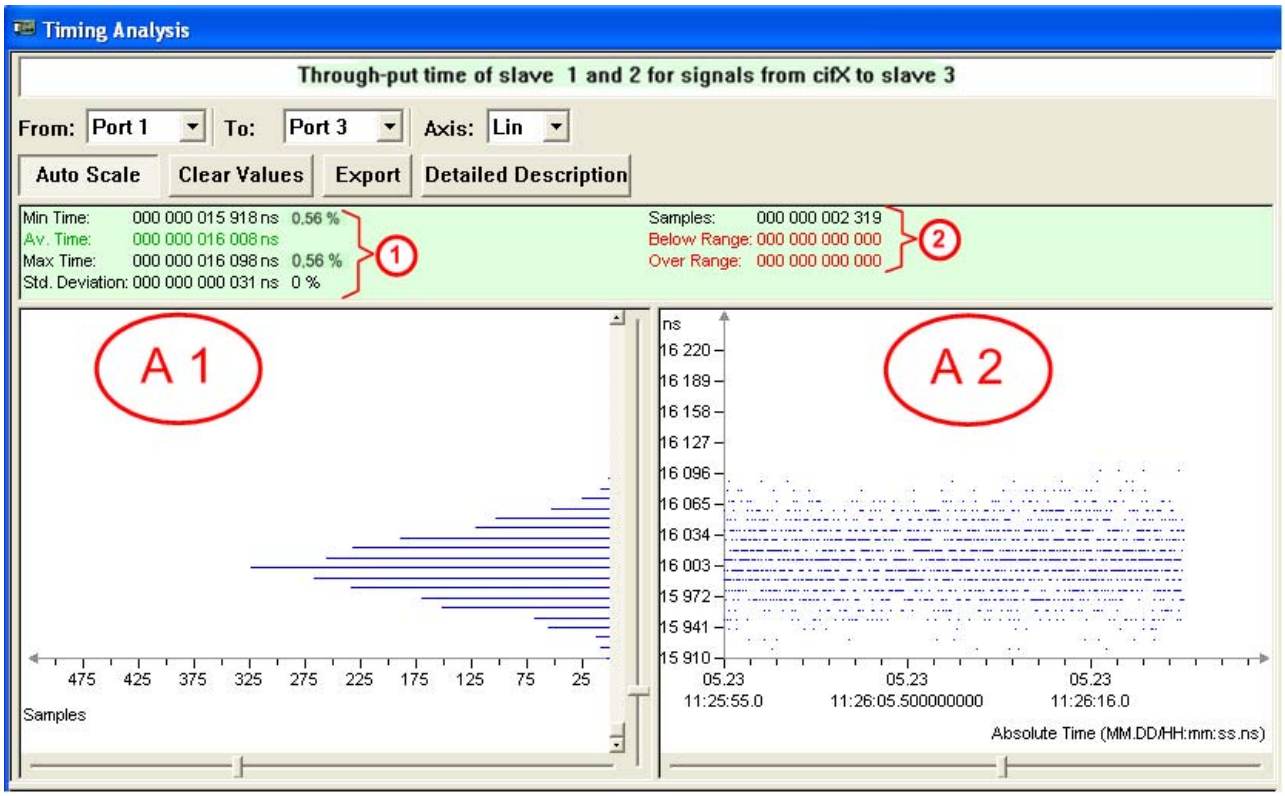


Abbildung 117: Modbus/TCP netANALYZER Analyse Fenster A

Im Fenster „**A 1**“ (dem Histogramm) sieht man die zeitliche Verteilung der einzelnen Telegramme und deren Anzahl.

Im Fenster „**A 2**“ (der Historie) sieht man die Verteilung der Telegramme über die Zeit.

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Durchlaufzeit, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	15,918 µs
Av Time	Die mittlere Durchlaufzeit der Telegramme.	16,008 µs
Max Time	Die maximale Durchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	16,098 µs
Std. Deviation	Die Standardabweichung der Durchlaufzeit.	31 ns

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	2319
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

8.2.4.2 Im Fenster B: Antwortzeit

Im Fenster B des Timing Analysis-Fensters finden Sie jetzt die Antwortzeit von Slave 3 auf die FC 4 Anfragen der cifX.

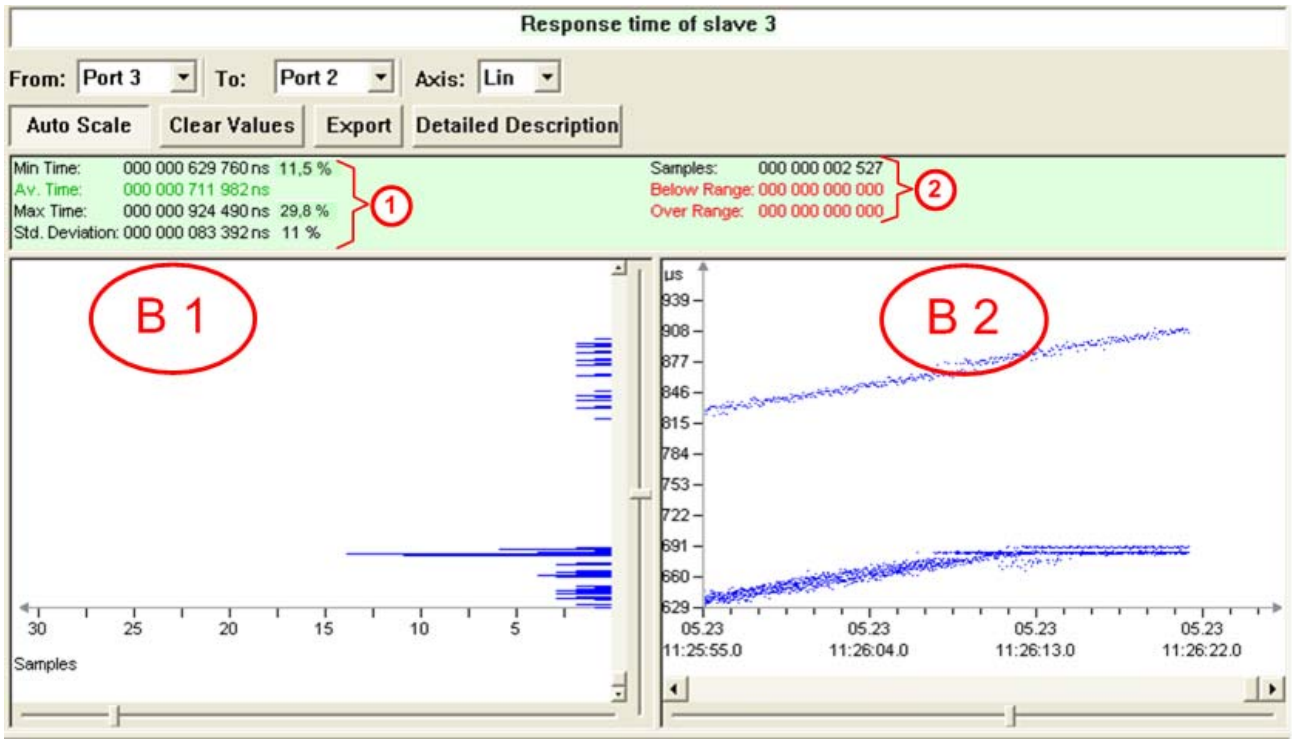


Abbildung 118: Modbus/TCP netANALYZER Analyse Fenster B

Im Fenster „**B 1**“ (dem Histogramm) sieht man die zeitliche Verteilung der einzelnen Telegramme und deren Anzahl.

Im Fenster „**B 2**“ (der Historie) sieht man die Verteilung der Telegramme über die Zeit.

Lässt man die Analyse über eine längere Zeit laufen, so kann man im Historie Fenster „**B 2**“ ein Driften der Antwortzeit über die Zeit erkennen.

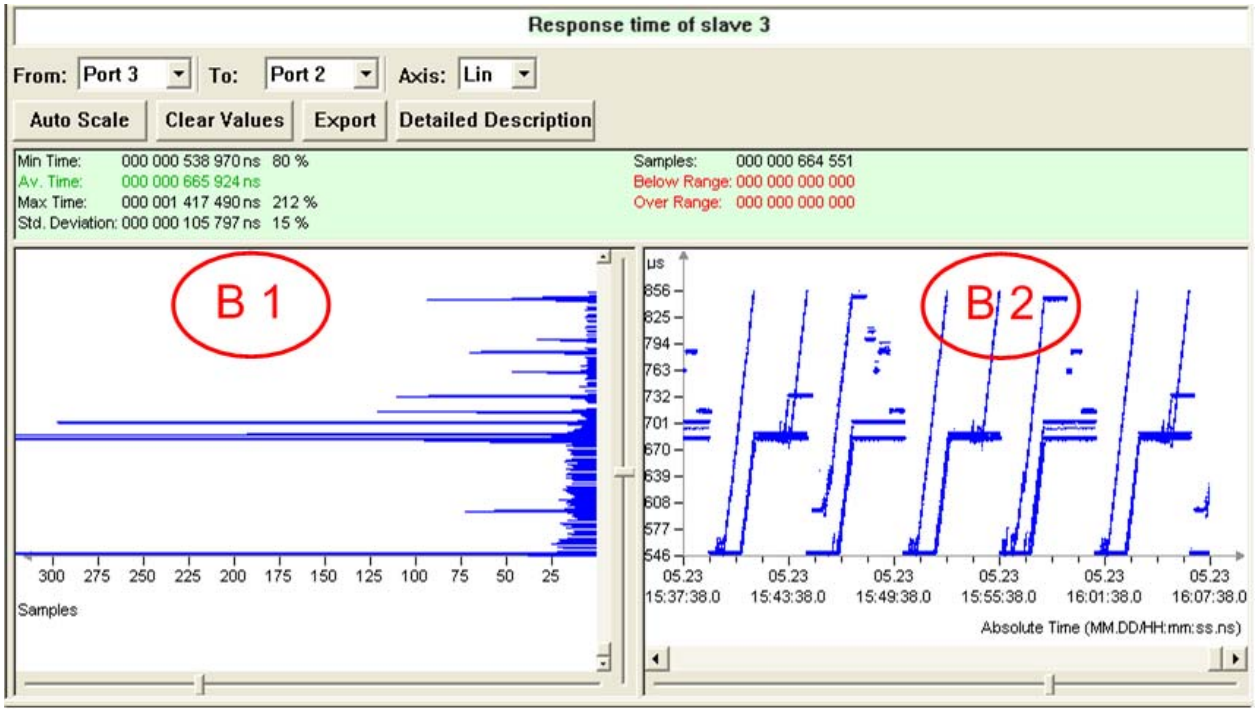


Abbildung 119: Modbus/TCP netANALYZER Analyse Fenster B

© Hilscher, 2008-2012

8.2.4.3 Im Fenster C: Durchlaufzeit

Im Fenster C des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

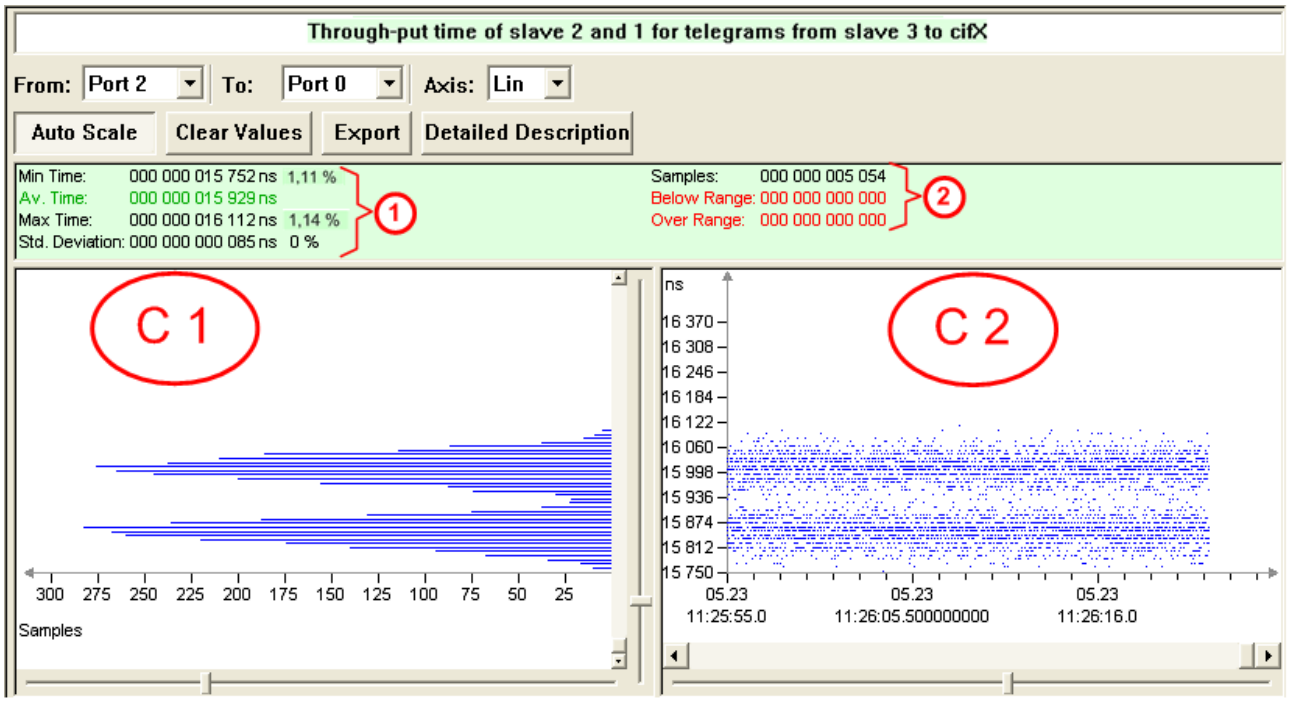


Abbildung 120: Modbus/TCP netANALYZER Analyse Fenster C

Hier sehen Sie die Durchlaufzeit der Antworttelegramme durch Slave 2 und Slave 1 auf die FC 4 Telegramme der PC-Karte cifX an den Slave (Server) 3.

Es ist deutlich zu sehen, dass es zwei maxima in der Streuung der Durchlaufzeit gibt, die jedoch über den zeitlichen Verlauf konstant ist.

Im Kopf des Messbildes sehen Sie folgende statistische Zahlen:

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Durchlaufzeit, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	15,752 µs
Av Time	Die mittlere Durchlaufzeit der Telegramme..	15,929 µs
Max Time	Die maximale Durchlaufzeit der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	16,112 µs
Std. Deviation	Die Standardabweichung der Durchlaufzeit.	85 ns

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	5054
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

8.2.4.4 Im Fenster D: Zykluszeit

Im Fenster D des Timing Analysis-Fensters finden Sie jetzt folgende Informationen:

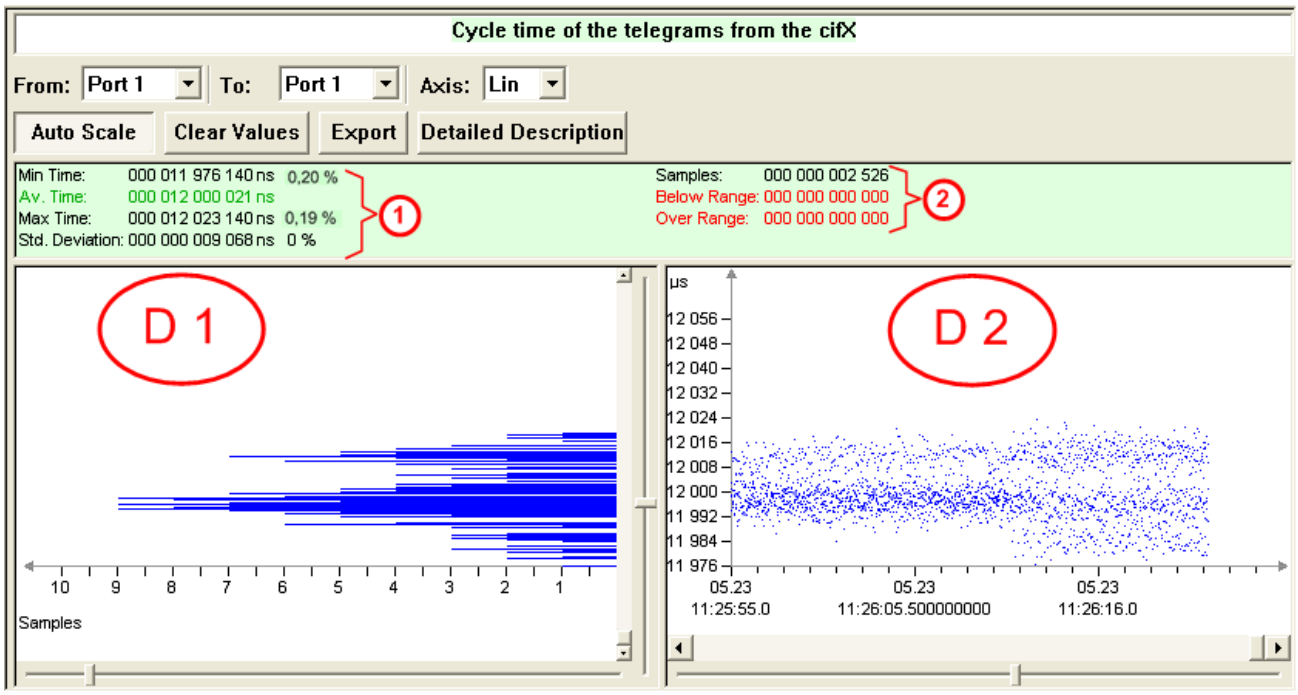


Abbildung 121: Modbus/TCP netANALYZER Analyse Fenster D

Hier sehen Sie die Zykluszeit, mit der die FC 4 Telegramme der PC-Karte cifX an den Slave (Server) 3 versendet werden.

Im Fenster „**D 2**“ kann man erkennen, dass die Streuung der Zykluszeit über die Zeit konstant ist.

Im Kopf des Messbildes sehen Sie folgende statistische Zahlen:

Bei ① sieht man unter:

Bezeichnung	Bedeutung	Wert
Min Time	Die minimale Zykluszeit, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	11,976 ms
Av Time	Die mittlere Zykluszeit, der Telegramme..	12,000 ms
Max Time	Die maximale Zykluszeit, der Telegramme, sowie die prozentuale Abweichung zur mittleren Durchlaufzeit.	12,023 ms
Std. Deviation	Die Standardabweichung der Zykluszeit,.	9,068 µs

Bei ② sieht man unter:

Bezeichnung	Bedeutung	Wert
Samples	Die Anzahl der ausgewerteten Telegramme.	2526
Below Range	Die Anzahl der Telegramme, die unterhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0
Over Range	Die Anzahl der Telegramme, die oberhalb der angezeigten Zeitspanne (Y-Achse) liegen.	0

© Hilscher, 2008-2012

8.3 Datenaufzeichnung durchführen

Es sollen die Telegramme der PC-Karte cifX zum Slave 3 und die Antworttelegramme vom Slave 3 an die PC-Karte cifX aufgezeichnet werden.

Voraussetzungen:

- Der Hardware-Aufbau wie im Abschnitt *Hardware-Aufbau* auf Seite 102 beschrieben muss erstellt sein,
- die Modbus-Mastersoftware muss gestartet und mit dem Slave 3 verbunden sein.

Hinweis: Bei der Telegrammaufzeichnung sind nur die Einstellungen der Hardwarefilter aktiv.

➢ Starten Sie die netANALYZER Software mit **Start > Programme > Hilscher GmbH > Hilscher netANALYZER.**

↬ Sie gelangen in das Hauptfenster des netANALYZERs.

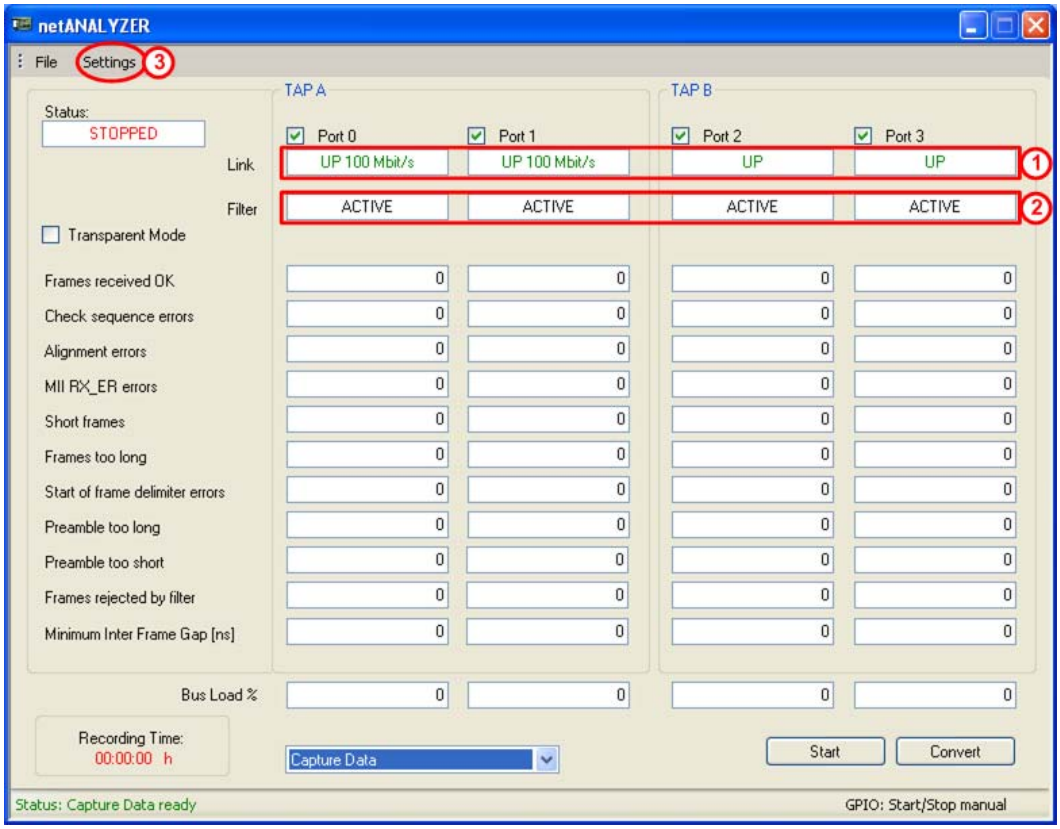


Abbildung 122: Modbus/TCP netANALYZER Analyse Start

Wenn Sie die Verkabelung (wie in Abschnitt *Hardware-Aufbau* auf Seite 102 beschrieben) aufgebaut haben und die Kommunikation zwischen der PC-Karte cifX und den NXIO-Boards läuft, wird der jeweilige Verbindungsstatus (wie bei ① dargestellt) als **UP** gekennzeichnet.

➢ Stellen Sie sicher, dass unter dem Dialogweg (wie bei ② dargestellt) **Settings > Filter Settings**, wie bei der Zeitmessung in Abschnitt *Zeitmessung vorbereiten* auf Seite 102 beschrieben, aktiviert sind.

➢ Verlassen Sie die Filtereinstellung mit **OK**.

↬ Sie kommen zurück ins Hauptfenster.

© Hilscher, 2008-2012

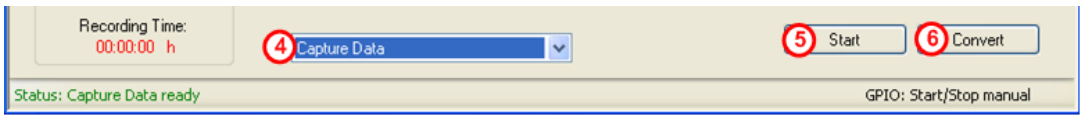


Abbildung 123: Datenaufzeichnung starten

- Stellen Sie sicher, dass **Capture Data** (4) eingestellt ist.
- Klicken Sie **Start** (5), um die Aufzeichnung zu starten.
- Die Schaltfläche **Start** (5) wird zur Schaltfläche **Stop** (5).
- Warten Sie bis eine ausreichende Anzahl von Telegrammen aufgezeichnet wurden.
- Klicken Sie **Stop** (5).
- Klicken Sie **Convert** (6).
- Es erscheint folgendes Fenster:

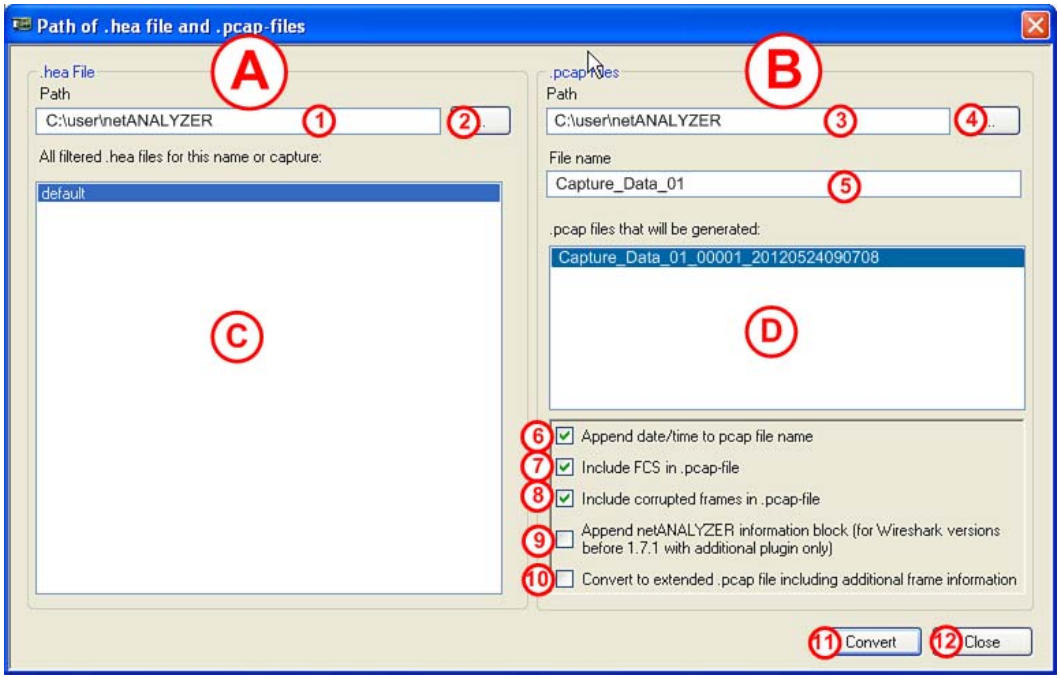


Abbildung 124: pcap-Konvertierung 1

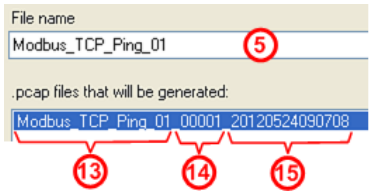
Das obige Fenster teilt sich in zwei Bereiche:

Fensterbereich (A)

Bedienelement	Erläuterung
Path (1)	Vom Bediener auszuwählender Pfad, aus welchem der netANALYZER die Binär-Datei (**.hea*) zur Konvertierung lesen soll. Die hier gemachten Einstellungen wirken sich auch auf die nächsten Datenaufzeichnungen aus. Die Einstellung unter **Settings > File Settings** wird damit verändert.
Schaltfläche (2)	Auswahlschaltfläche zur Auswahl des Quellverzeichnisses der .hea-Dateien.
All filtered .hea files for this name or capture (C)	Anzeigeliste der .hea-Dateien im ausgewähltem Verzeichnis

© Hilscher, 2008-2012

Fensterbereich B

Bedienelement	Erläuterung
Path 3	Der vom Bediener zu definierende Pfad, unter welchem die **netANALYZER**-Software die konvertierte WinPcap-Datei (**.pcap*) ablegen soll.
Schaltfläche 4	Auswahlschaltfläche zur Auswahl des Zielverzeichnis der .pcap-Dateien.
File name 5	Systematische Dateibezeichnung für die **.pcap*-Dateien. Die **netANALYZER**-Software vergibt zusätzlich für jede Datei noch eine fortlaufende Nummer im Dateinamen.
.pcap files that will be generated D	Vorschau der zu erzeugenden **.pcap*-Dateien. Dabei ist der Namensaufbau wie folgt:  13 der unter 5 ausgewählte Dateiname. 14 laufende Zählnummer 15 Zeitinformation, bestehend aus: yyyymmddhhmmss (Beginn der Aufzeichnung der hea-Datei, (nur wenn 6 der Haken gesetzt wurde.).
Append date/time to pcap file name 6	Ist der Haken gesetzt, werden Datum und Zeit im Dateinamen ergänzt.
Include FCS in .pcap-files 7	Checkbox ob die Ethernet-Prüfsumme mit in der PCAP-Datei enthalten sein soll oder nicht. (Einige Wireshark-Dissectoren unterstützen FCS nicht.) **Hinweis:** Wenn **Convert to extended .pcap file including additional frame information** angehakt ist, ist **Include FCS in .pcap-file** ausgegraut, da FCS dann immer in eine .pcap-Datei konvertiert wird. FCS = Frame Check Sequence (Ethernet-Prüfsumme) Nicht auswählbar, wenn Option 10 angehakt, jedoch aktiv.
Include corrupted frames in .pcap file 8	Ist diese Option aktiviert, werden auch fehlerhafte Frames in die .pcap-Datei übernommen. Ist die Option deaktiviert werden nur korrekte Telegramme in der .pcap-Datei gespeichert.
Append netANALYZER information block (for Wireshark versions before 1.7.1 with additional plug in only) 9	Die Option erfordert für Wireshark-Versionen < V1.7.1 die Installation des netANALYZER-Wireshark-Plugins. Fügt den netANALYZER-Info-Block nach dem Ethernet-Frame in die .pcap-Dateien ein. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen. **Hinweis:** Das .pcap-Dateiformat mit dem Info-Block nach dem Ethernet-Frame wird von Wireshark-Versionen ≥ 1.7.1 nicht mehr unterstützt. Nicht auswählbar, wenn Option 10 angehakt.
Convert to extended .pcap file including additional frame information 10	**Hinweis:** Wird dieser Haken gesetzt, kann das mit der netANALYZER-Software V1.4.x.x erzeugte erweiterte .pcap-Dateiformat nur in Wireshark-Versionen ab V1.7.1 geöffnet werden. Ab der Version der netANALYZER-Software V1.4.x.x kann ein erweitertes .pcap-Dateiformat erzeugt werden. Dabei befindet sich der „netANALYZER Info-Block“ in den 4 Bytes vor dem Ethernet-Frame. Damit stehen Zusatzinformationen zu jedem einzelnen Telegramm zur Verfügung, wie Empfangszeitpunkt, Empfangs-Port oder Fehlerinformationen.
Convert 11	Die Konvertierung der Binär-Dateien ins WinPcap-Format wird gestartet.
Close 12	Sie schließen das Fenster ohne eine Konvertierung zu starten.

- Wählen Sie im Fensterbereich A die zu konvertierende Datei aus.
- Ergänzen Sie die notwendigen Einstellungen im Fensterbereich B.
- Klicken Sie auf die Schaltfläche **Convert** 11, um die Daten ins pcap-Format zu konvertieren.

Nach Abschluss des Konvertierungsvorgangs schließt sich das Fenster.

© Hilscher, 2008-2012

➢ Öffnen Sie die Datei mit Wireshark.
Wenn das Programm Wireshark korrekt installiert ist, wird mittels eines Doppelklicks auf die .pcap-Datei diese mit Wireshark geöffnet.

➢ Es werden folgende Daten angezeigt:

➢ Das Programm Wireshark zeigt die Daten wie folgt an:

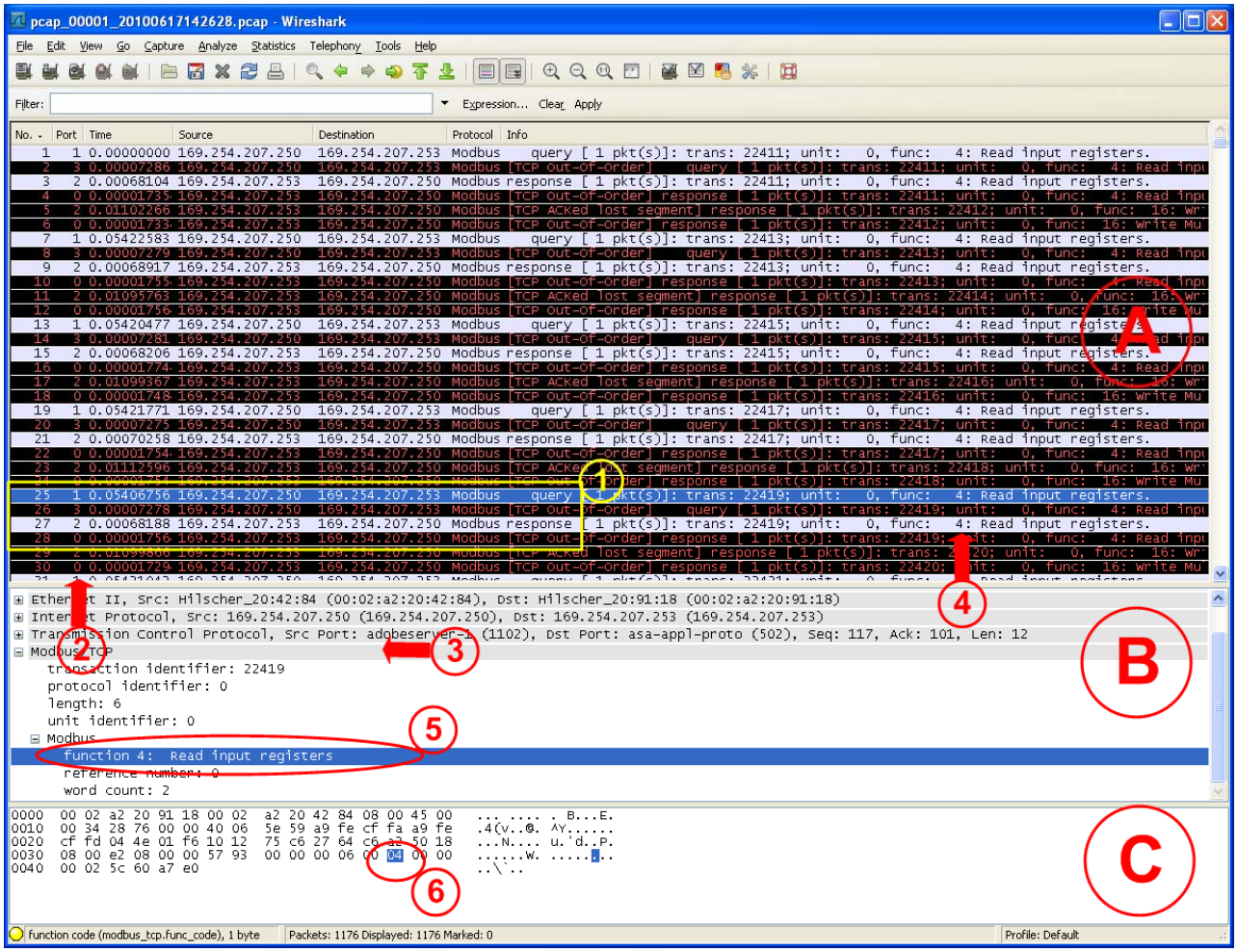


Abbildung 125: Modbus/TCP netANALYZER Wireshark Telegrammdarstellung

Ⓐ In diesem Fensterbereich sehen Sie die Auflistung aller entsprechend der Filtereinstellung detektierten Telegramme. Hier ist unter ② der Port der netANALYZER-Karte zu finden, über dem das Telegramm aufgezeichnet wurde.

Ⓑ In diesem Fensterbereich können Sie einzelne Telegrammbereiche des ausgewählten Telegramms betrachten. Hier sind unter ③ die einzelnen Modbus-Telegrammabschnitte aufzublättern.

Ⓒ In diesem Fensterbereich werden die Daten des ausgewählten Telegramms auf Byteebene dargestellt.

① Hier ist ein Telegrammzyklus zu sehen. Die aufgezeichneten Telegramme sind durchnummeriert.

Nr.	Port	Beschreibung
25	1	Der Zeitpunkt an dem das Telegramm (vom Master zum Slave) den PC verlässt.
26	3	Der Zeitpunkt an dem das Telegramm vor dem Slave 3 ist. Da der Telegramminhalt bereits aufgezeichnet wurde, wird dass Telegramm schwarz hinterlegt und mit [TCP-Out-of Order] gekennzeichnet.

© Hilscher, 2008-2012

Nr.	Port	Beschreibung
27	2	Der Zeitpunkt an dem das Antworttelegramm des Slaves an den Master den Slave verlässt.
28	0	Der Zeitpunkt an dem das Antworttelegramm des Slaves bei dem PC ankommt.

Da auf 2 TAPs aufgezeichnet wird, und durchlaufende Telegramme zwei mal erfasst werden, ist Wireshark nicht in der Lage die Reihenfolge der TCP Segmente zu prüfen.

Daher wird das Segment eines bereits aufgezeichneten Telegramms schwarz hinterlegt und mit [TCP-Out-of Order] gekennzeichnet.

⑤ Hier ist im Telegramm der Funktioncode (4) des Modbustelegramms ausgewählt, dessen Position auf Byteebene unter der Kennung ⑥ zu sehen ist.

8.4 Netzlast-Analyse vorbereiten und durchführen

Es soll die Netzlast zwischen Slave 2 und Slave 3 beim Anlauf der Netzwerkkommunikation ermittelt werden und die Belastung durch einen Ping-Aufruf zeigen.

8.4.1 Netzlast-Analyse vorbereiten

Sie können wie in Abschnitt *Datenaufzeichnung durchführen* auf Seite 116 beschrieben, für den Netzwerkanlauf ein Data-Capture durchführen, um die relevanten Daten für die Einstellungen zu ermitteln, oder vordefinierte Filter benutzen.

Wir wollen hier die bereits mitgelieferten Filtereinstellungen verwenden.

Hinweis: Bei der Netzlast-Analyse sind immer die **Extended Software Filter** aktiv..

8.4.2 Filter einstellen

➢ Hardware-Filter ausschalten

Abbildung 126: Hardware-Filter ausschalten

Hinweis: Die eingestellten Hardware (Standard-Filter) wirken Additiv zu dem *Extended Software Filter*. Aus diesem Grunde entfernen wir die Haken bei Enable Filter ① aus dem Hardware-Filter, oder den Haken bei *Select Filter* ②.

➢ Softwarefilter einstellen.

➢ Zur Konfiguration der *Extended Software Filter* gehen Sie wie folgt vor:

© Hilscher, 2008-2012

1. Rufen Sie im netANALYZER Hauptmenü unter **Settings > Extended Software Filter Settings** auf.

Es öffnet sich folgendes Konfigurationsfenster:

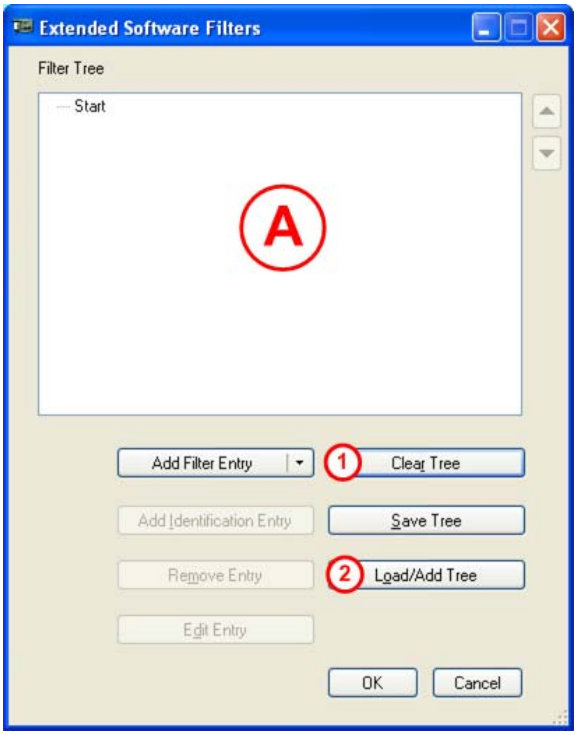


Abbildung 127: Extended Software Filters

Sollte der Bereich nicht so leer, sein wie in der obigen Abbildung dargestellt, klicken Sie **Clear Tree** ①, um die Filtereinstellungen zu löschen.

- Klicken Sie **Load/Add Tree** ②, um einen Filter auszuwählen.
  - Es öffnet sich der Dateimanager des Betriebssystems mit dem Verzeichnis der vordefinierten Filter.
- Wählen Sie die Datei `MODBUS_frame.xml` aus. In diesem Filter sind bereits alle Einstellungen für die zyklische Kommunikation an einem Modbus/TCP-Netzwerk vorhanden.

Das Extended Software Filter solle nach dem Aufklappen aller Untereinträge wie folgt aussehen.

© Hilscher, 2008-2012

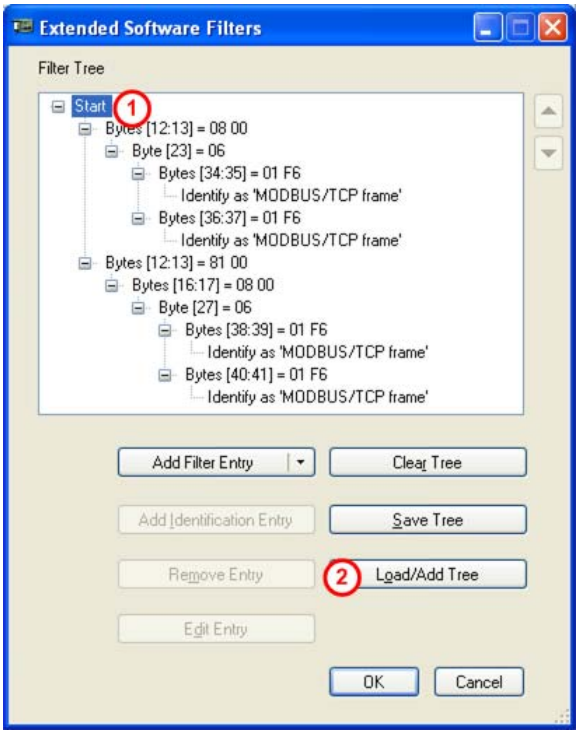


Abbildung 128: Extended Software Filters für zyklische Modbus/TCP Telegramme

Zusätzlich sollen die Ping-Aufrufe auf dem Netzwerk gefiltert werden. Dazu muss dem obigem Filter ein weiterer hinzugefügt werden.

- Markieren Sie den Eintrag **Start** (1) entsprechend der obigen Abbildung, um eine ODER-Verknüpfung zu dem bereits ausgewählten Filter zu erzeugen.
- Klicken Sie **Load/Add Tree** (2) um einen weiteren Filter auszuwählen.
- Es öffnet sich der Dateimanager des Betriebssystems mit dem Verzeichnis der vordefinierten Filter.
- Wählen Sie die Datei `ICMP_frame.xml` aus. In diesem Filter sind auch die Einstellungen für einen Ping-Aufruf enthalten.
- Das Extended Software Filter solle nach dem Aufklappen aller untereinträge jetzt wie folgt aussehen.

© Hilscher, 2008-2012

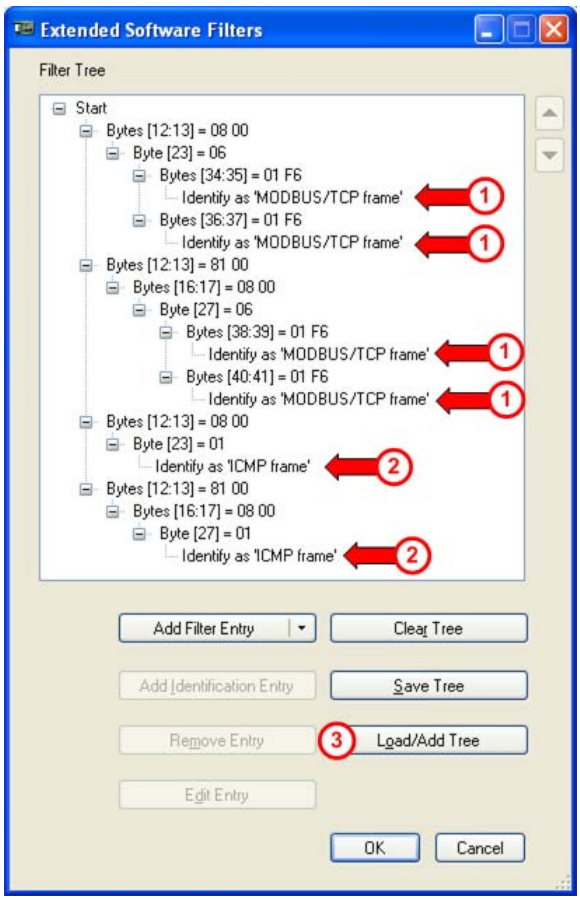


Abbildung 129: Extended Software Filters für zyklische Modbus/TCP Telegramme und Ping

Für jeden Eintrag mit **Identify as** wird ein Zählertopf für die Analyse eröffnet. Da der Name **Identify as MODBUS/TCP frame** (1) vier mal vorkommt, werden alle diese Filterergebnisse in dem selben Zählertopf gezählt. Dieses gilt ebenso für den Zählertopf **Identify as ICMP frame** (für den Ping-Aufruf), der zwei Quellen hat.

Hinweis: Treten bei der Telegrammanalyse noch andere Datensätze auf, die nicht den Filterbedingungen entsprechen, wird der Analyse automatisch der Topf **Other** hinzugefügt.

- ➢ Speichern Sie die Filtereinstellungen für spätere Anwendungen. Verlassen Sie mit **OK** (3) das Filterfenster.
- ➢ Sie gelangen zurück in das Hauptfenster des netANALYZERs.

© Hilscher, 2008-2012

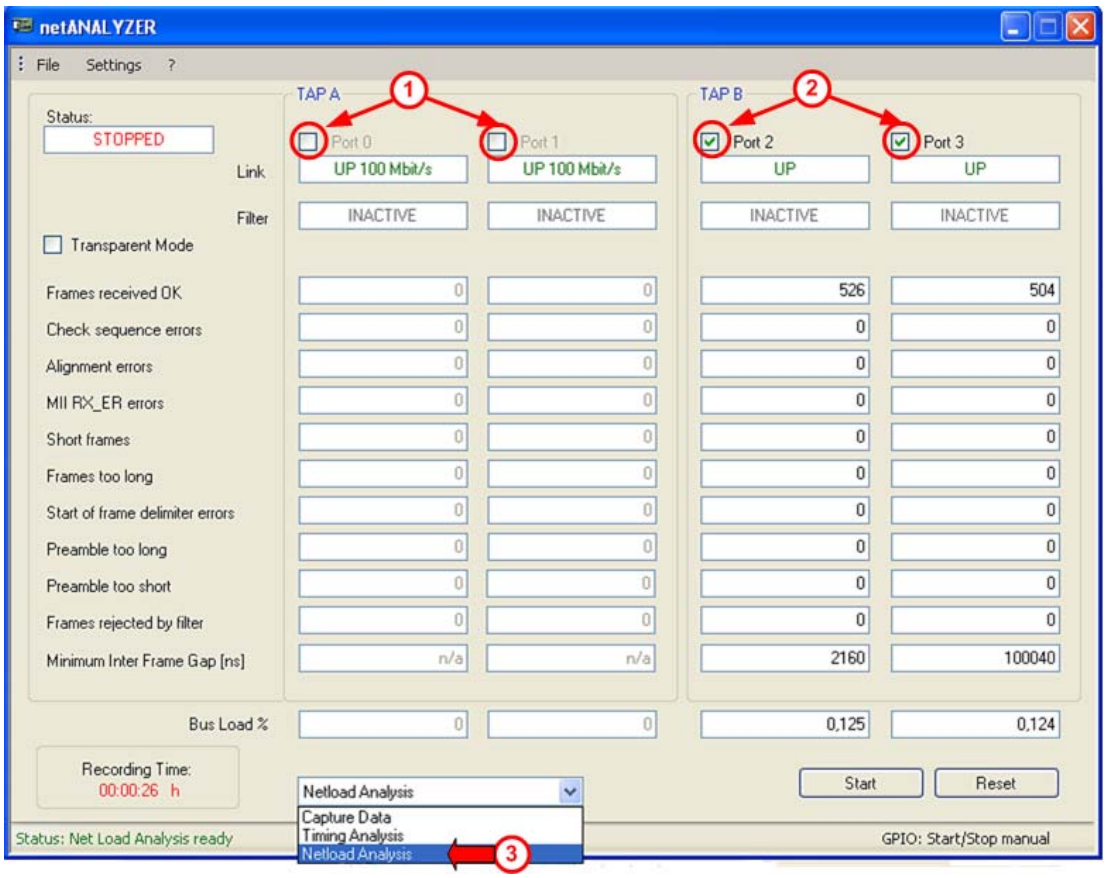


Abbildung 130: netANALYZER Hauptfenster Modbus/TCP Netload Analyse

- Setzen Sie den Haken bei TAP B für Port 2 und Port 3 (2).
  Dieses ist erforderlich, da wegen der Auto Cross Over Funktionalität der Ethernetanschlüsse nicht vorhersehbar ist, über welchen Port die Kommunikation startet.
- Entfernen Sie ggf. die Haken bei TAP A (1), um die dort erfassten Telegramme nicht in der Messung zu berücksichtigen.

8.4.3 Netzlastmessung durchführen

- Wählen Sie für die Analyse **Netload Analysis** (3).
- Es öffnet sich das Netload Analysis Fenster.
- Öffnen Sie die Ethernetverbindung am CH 0 des Slave 1 der *Abbildung 103*, um sie nach dem Start der Analyseaufzeichnung wieder schließen zu können, damit die nicht Modbus/TCP Telegramme beim Verbindungsaufbau erfasst werden können.
- Wählen Sie das Hauptfenster des netANALYZER an.
- Klicken Sie **Start**.
- Die Datenaufzeichnung beginnt.
- Schließen Sie das Kabel am CH 0 des Slaves wieder an.
- Stoppen Sie nach einiger Zeit der Aufzeichnung mit **Stop** im Hauptfenster des netANALYZERs.
- Im Netload Analysis Fenster sehen Sie jetzt etwa folgende Informationen:

© Hilscher, 2008-2012

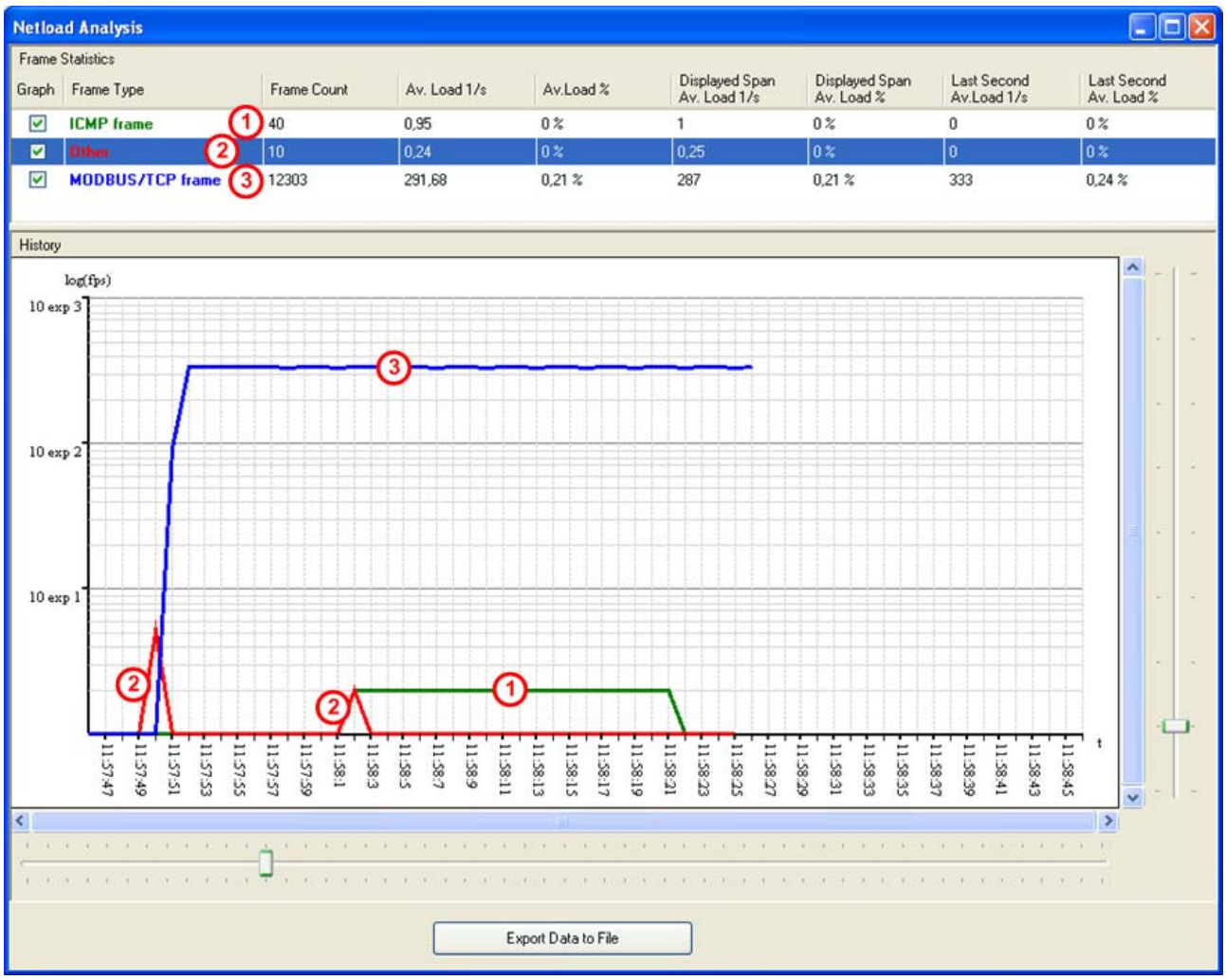


Abbildung 131: Netzlast für zyklische MODBUS/TCP Telegramme (Anlauf) und Ping

In der obigen Abbildung ist zu sehen, dass es nach einer Netzwerkunterbrechung, zu Beginn der Kommunikation, einige nicht Modbus/TCP-Telegramme (Kurve ②) gibt, und die Modbus/TCP -Kommunikation (Kurve ③) ca. 1 sec. nach Behebung der Unterbrechung beginnen.

Die Ping-Aufrufe wurden am CH 1 des Slave 3 eingespeist und waren an den Slave 1 adressiert. Der Ping-Aufruf wurde 20 mal wiederholt (Kurve ①). Der erste Ping-Aufruf wird mit einem ARP-Telegramm eingeleitet. Daher gibt es hier auch einen Peak beim Telegrammtopf **Other**.

Wird die Modbus/TCP-Kommunikation nicht durch Netzwerkunterbrechung neu gestartet, sondern durch eine Spannungswiederkehr der Slaves, ist die nicht Modbus/TCP-Kommunikation vor dem Start der selbigen noch umfangreicher, da dann noch die Kommunikation für die Adressverteilung über den DHCP-Server dazukommt. Dieser Fall wird in der folgenden Abbildung dargestellt.

© Hilscher, 2008-2012

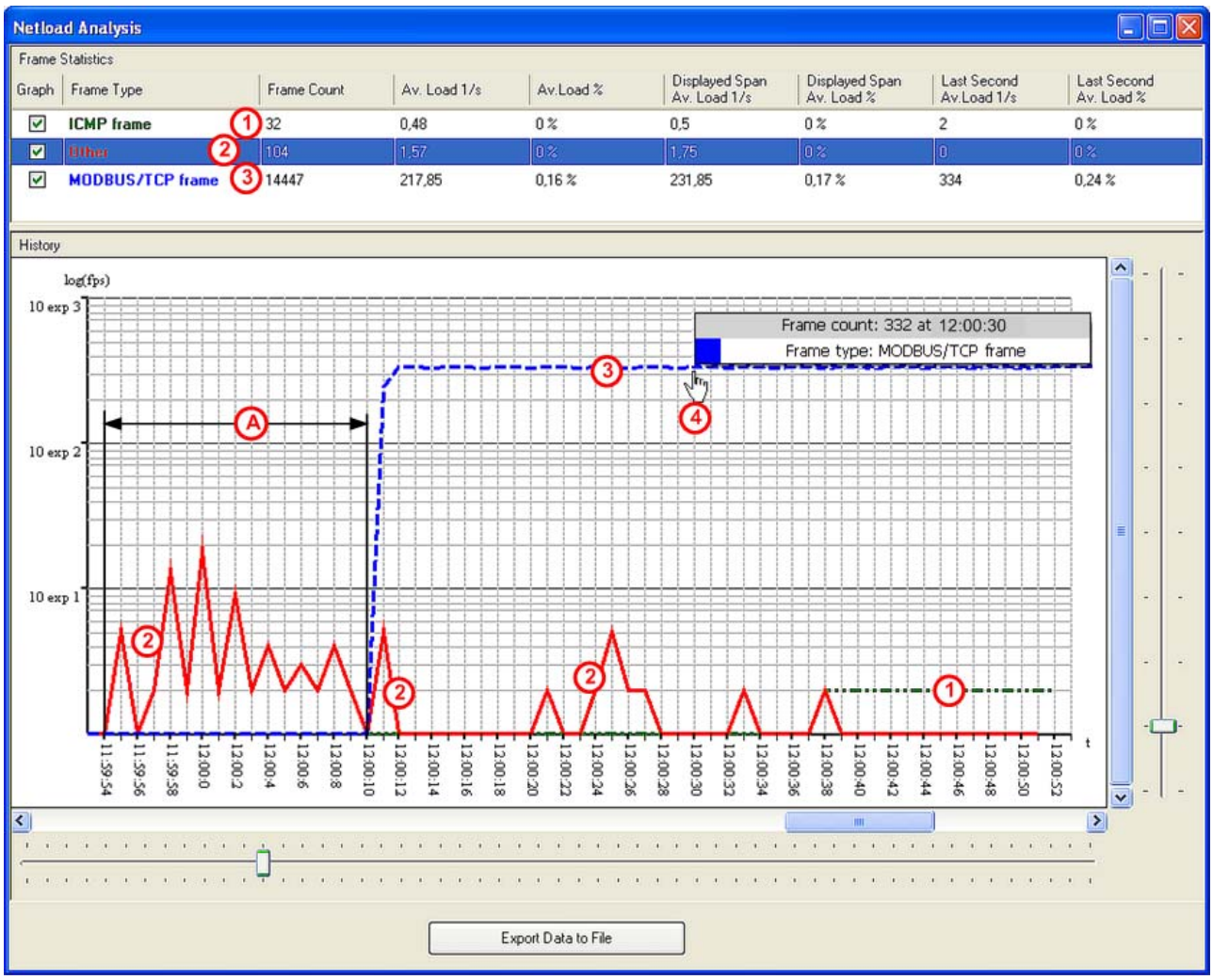


Abbildung 132: Netzlast für zyklische Modbus/TCP-Telegramme (Anlauf nach Spannungswiederkehr)

In der obigen Abbildung kommen die nicht Modbus-Telegramme im Zeitraum Ⓐ überwiegend von der Adresszuteilung der Slaves über den DHCP-Server und dem Test auf identische Adressen im Netzwerk. Der Start der zyklischen Modbus/TCP-Kommunikation erfolgt ca. 13 sec. nach der Spannungswiederkehr. Sind mehr Teilnehmer am Netzwerk vorhanden, wird sich dieser Zeitabschnitt noch vergrößern.

Fahren Sie mit dem Mauszeiger entlang einer Messlinie in der Grafik ④, verändert sich der Mauszeiger zur Hand und es wird die Anzahl der Telegramme, die pro Sekunde für diesen Filter gezählt wurden angezeigt.

© Hilscher, 2008-2012

9 Glossar

CSV

Comma Separated Value

FCS

Frame Check Sequence (Prüfsumme am Frame-Ende zur Fehlererkennung)

GPIO

General Purpose Input/Output

hea

Dateiendung der von der Hilscher netANALYZER-Software erzeugten Binär-Datei (default.hea) mit dem Capture-Informationsgehalt

.NET Framework Version 2.0

Microsoft .NET Framework Version 2.0
http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=de

PIO

Programmable Input/Output

TAP

Test Access Point

Wireshark

„Netzwerk-Monitoring Programm Wireshark“
http://www.wireshark.org

WinPcap

„Die Library WinPcap“
http://www.winpcap.org/

© Hilscher, 2008-2012

10 Anhang

10.1 Abbildungsverzeichnis

Abbildung 1: netANALYZER Startbild 12
Abbildung 2: netANALYZER File Settings 13
Abbildung 3: Timing-Analyse, Skalierung ändern 14
Abbildung 4: Timing Analyse, zoomen mit der Maus 15
Abbildung 5: PROFINET IO Analyse, Hardware-Aufbau 16
Abbildung 6: netANALYZER Hauptfenster 17
Abbildung 7: netANALYZER Filtereinstellungen (1) 18
Abbildung 8: netANALYZER Filtereinstellungen (2) 19
Abbildung 9: netANALYZER, Auswahl Timing-Analyse 21
Abbildung 10: netANALYZER Messfenster 22
Abbildung 11: netANALYZER, Hauptfenster nach Messzyklus 23
Abbildung 12: netANALYZER Messfenstereinstellungen 1 24
Abbildung 13: netANALYZER Messfenstereinstellungen 2 24
Abbildung 14: netANALYZER Hauptfenster, Start, Reset 25
Abbildung 15: netANALYZER PROFINET IO Zykluszeitmessung, Auto-Scale 25
Abbildung 16: PROFINET IO, Device 1 Durchlaufzeit 26
Abbildung 17: PROFINET IO, Device 1 Durchlaufzeit, History extrem gespreizt 27
Abbildung 18: Hauptfenster für Telegrammaufzeichnung 28
Abbildung 19: netANALYZER PROFINET IO Filtereinstellungen 29
Abbildung 20: Datenaufzeichnung starten 30
Abbildung 21: pcap-Konvertierung 1 30
Abbildung 22: Telegrammdarstellung in Wireshark 32
Abbildung 23: Standard PROFINET Datensatz 34
Abbildung 24: Hardware-Filter ausschalten 35
Abbildung 25: Extended Software Filter erstellen (1) 35
Abbildung 26: Extended Software Filter erstellen (2) 36
Abbildung 27: Extended Software Filter nach 1. Eintrag 36
Abbildung 28: Extended Software Filter nach 2. Eintrag 37
Abbildung 29: Extended Software Filter nach 3. Eintrag 38
Abbildung 30: netANALYZER Hauptfenster PROFINET Netload Analyse 38
Abbildung 31: Netload Analyse für PROFINET Anlaufphase 39
Abbildung 32: Extended Software Filter mit FrameID 40
Abbildung 33: Netload Analyse für PROFINET Anlaufphase mit FrameID 8002 41
Abbildung 34: EtherCAT Hardware-Aufbau 42
Abbildung 35: netANALYZER Hauptfenster 43
Abbildung 36: netANALYZER Filterfenster 44
Abbildung 37: netANALYZER Timing-Analyse-Fenster 45
Abbildung 38: netANALYZER Timing-Auto-Scale 45
Abbildung 39: Timing-Analysefenster A, EtherCAT Zykluszeit 46
Abbildung 40: Timing-Analysefenster B, EtherCAT Ringdurchlaufzeit (1) 46
Abbildung 41: Timing-Analysefenster C, EtherCAT Ringdurchlaufzeit (2) 47
Abbildung 42: Timing-Analysefenster D, EtherCAT Ringdurchlaufzeit (2) 47
Abbildung 43: netANALYZER Start / Stopp Analyse 47
Abbildung 44: EtherCAT Timing-Analysefenster A mit Messdaten 48
Abbildung 45: EtherCAT Timing-Analysefenster B mit Messdaten 49
Abbildung 46: EtherCAT Timing-Analysefenster C mit Messdaten 51
Abbildung 47: EtherCAT Timing-Analysefenster D mit Messdaten 52
Abbildung 48: EtherCAT netANALYZER Hauptfenster 53
Abbildung 49: Datenaufzeichnung starten 54
Abbildung 50: pcap-Konvertierung 1 54
Abbildung 51: EtherCAT Wireshark Daten 56
Abbildung 52: EtherNet/IP Hardware-Aufbau 58
Abbildung 53: EtherNet/IP Filter Data Capture 59

© Hilscher, 2008-2012

Abbildung 54: EtherNet/IP Data Capture Start 60
Abbildung 55: Ethernet/IP netANALYZER Analyse Convertierung 1 61
Abbildung 56: EtherNet/IP Data Capture 63
Abbildung 57: EtherNet/IP netANALYZER Hauptfenster 65
Abbildung 58: EtherNet/IP netANALYZER Filter cifX → Slave 3 66
Abbildung 59: EtherNet/IP netANALYZER Signalflussrichtung 67
Abbildung 60: EtherNet/IP netANALYZER Filter Slave 3 → cifX 68
Abbildung 61: netANALYZER Timing-Analyse-Fenster 69
Abbildung 62: netANALYZER Timing-Auto-Scale 70
Abbildung 63: EtherNet/IP Porteinstellungen für Zykluszeit, Timingfenster A 70
Abbildung 64: EtherNet/IP Porteinstellungen für Antwortzeit Slave 3, Timingfenster B 70
Abbildung 65: EtherNet/IP Porteinstellungen für Durchlaufzeit zum Slave 3, Timingfenster C 71
Abbildung 66: EtherNet/IP Porteinstellungen für Durchlaufzeit durch Slave 1 und 2 zur cifX, Timingfenster D 71
Abbildung 67: Hauptfenster des netANALYZERs 71
Abbildung 68: EtherNet/IP, Zykluszeit cifX→ Slave 3 72
Abbildung 69: EtherNet/IP, Durchlaufzeit cifX -> Slave3 durch Slave 1 und 2 73
Abbildung 70: EtherNet/IP, Zykluszeit des Slave 3 74
Abbildung 71: EtherNet/IP, Durchlaufzeit Slave 2 und 1 Slave 3 → cifX 75
Abbildung 72: netANALYZER Einstiegsfenster 76
Abbildung 73: Datenaufzeichnung starten 77
Abbildung 74: pcap-Konvertierung 1 77
Abbildung 75: EtherNet/IP, Wireshark Telegrammanzeige 79
Abbildung 76: Hardware-Filter ausschalten 80
Abbildung 77: Extended Software Filters 81
Abbildung 78: Extended Software Filters für zyklische Ethernet/IP Telegramme 82
Abbildung 79: Extended Software Filters für zyklische Ethernet/IP-Telegramme und Ping 83
Abbildung 80: netANALYZER Hauptfenster Ethernet/IP Netload Analyse 84
Abbildung 81: Netzlast für zyklische Ethernet/IP Telegramme (Anlauf) und Ping 85
Abbildung 82: Netzlast für zyklische Ethernet/IP Telegramme (Anlauf nach Spannungswiederkehr) 86
Abbildung 83: sercos, Hardware-Aufbau 87
Abbildung 84: netANALYZER Einstiegsfenster 88
Abbildung 85: netANALYZER Sercos Filtereinstellungen 89
Abbildung 86: netANALYZER Sercos GPIO Settings 90
Abbildung 87: netANALYZER Timing-Analyse-Fenster 90
Abbildung 88: netANALYZER Timing-Auto-Scale 91
Abbildung 89: netANALYZER Port-Selektion 91
Abbildung 90: Sercos Einstellungen Timinganalysefenster A 91
Abbildung 91: Sercos Einstellungen Timinganalysefenster B 92
Abbildung 92: Sercos Einstellungen Timinganalysefenster C 92
Abbildung 93: Sercos Einstellungen Timinganalysefenster D 92
Abbildung 94: netANALYZER Start Analysezyklus 93
Abbildung 95: netANALYZER Ring-Delay Zeit 93
Abbildung 96: netANALYZER ConClk Zykluszeit am Slave 1 94
Abbildung 97: Zykluszeit Master-Daten-Telegramm Ausgang Master 95
Abbildung 98: Zykluszeit Master-Daten-Telegramm nach Durchlauf von 3 Slaves 96
Abbildung 99: netANALYZER Hauptfenster 98
Abbildung 100: Datenaufzeichnung starten 99
Abbildung 101: pcap-Konvertierung 1 99
Abbildung 102: SERCOS III Wireshark Telegrammdarstellung 101
Abbildung 103: Modbus/TCP Hardware-Aufbau 102
Abbildung 104: Modbus/TCP netANALYZER Start 103
Abbildung 105: Modbus/TCP netANALYZER Filter 1 104
Abbildung 106: Modbus/TCP netANALYZER Filter 1 Test 105
Abbildung 107: Modbus/TCP netANALYZER Filter 2 106
Abbildung 108: Modbus/TCP netANALYZER Filter 3 107
Abbildung 109: Modbus/TCP netANALYZER Start Timing Analyse 108

© Hilscher, 2008-2012

Abbildung 110: netANALYZER Timing-Analyse-Fenster 108
Abbildung 111: netANALYZER Timing-Auto-Scale 109
Abbildung 112: Modbus/TCP netANALYZER Messfenstereinstellungen 1 109
Abbildung 113: Modbus/TCP netANALYZER Messfenstereinstellungen 2 110
Abbildung 114: Modbus/TCP netANALYZER Messfenstereinstellungen 3 110
Abbildung 115: Modbus/TCP netANALYZER Messfenstereinstellungen 4 110
Abbildung 116: Modbus/TCP netANALYZER Start / Stopp Analyse 111
Abbildung 117: Modbus/TCP netANALYZER Analyse Fenster A 112
Abbildung 118: Modbus/TCP netANALYZER Analyse Fenster B 113
Abbildung 119: Modbus/TCP netANALYZER Analyse Fenster B 113
Abbildung 120: Modbus/TCP netANALYZER Analyse Fenster C 114
Abbildung 121: Modbus/TCP netANALYZER Analyse Fenster D 115
Abbildung 122: Modbus/TCP netANALYZER Analyse Start 116
Abbildung 123: Datenaufzeichnung starten 117
Abbildung 124: pcap-Konvertierung 1 117
Abbildung 125: Modbus/TCP netANALYZER Wireshark Telegrammdarstellung 119
Abbildung 126: Hardware-Filter ausschalten 120
Abbildung 127: Extended Software Filters 121
Abbildung 128: Extended Software Filters für zyklische Modbus/TCP Telegramme 122
Abbildung 129: Extended Software Filters für zyklische Modbus/TCP Telegramme und Ping 123
Abbildung 130: netANALYZER Hauptfenster Modbus/TCP Netload Analyse 124
Abbildung 131: Netzlast für zyklische MODBUS/TCP Telegramme (Anlauf) und Ping 125
Abbildung 132: Netzlast für zyklische Modbus/TCP-Telegramme (Anlauf nach Spannungswiederkehr) 126

10.2 Tabellenverzeichnis

Tabelle 1: Änderungsübersicht 4
Tabelle 2: Übersicht der Messbeispiele 10
Tabelle 3: Beschreibung File Settings 13

© Hilscher, 2008-2012

10.3 Kontakte

Hauptsitz

Deutschland
Hilscher Gesellschaft für
Systemautomation mbH
Rheinstrasse 15
65795 Hattersheim
Telefon: +49 (0) 6190 9907-0
Fax: +49 (0) 6190 9907-50
E-Mail: info@hilscher.com

Support
Telefon: +49 (0) 6190 9907-99
E-Mail: de.support@hilscher.com

Niederlassungen

China
Hilscher Systemautomation (Shanghai) Co. Ltd.
200010 Shanghai
Telefon: +86 (0) 21-6355-5161
E-Mail: info@hilscher.cn

Support
Telefon: +86 (0) 21-6355-5161
E-Mail: cn.support@hilscher.com

Frankreich
Hilscher France S.a.r.l.
69500 Bron
Telefon: +33 (0) 4 72 37 98 40
E-Mail: info@hilscher.fr

Support
Telefon: +33 (0) 4 72 37 98 40
E-Mail: fr.support@hilscher.com

Indien
Hilscher India Pvt. Ltd.
New Delhi - 110 065
Telefon: +91 11 43055431
E-Mail: info@hilscher.in

Italien
Hilscher Italia S.r.l.
20090 Vimodrone (MI)
Telefon: +39 02 25007068
E-Mail: info@hilscher.it

Support
Telefon: +39 02 25007068
E-Mail: it.support@hilscher.com

Japan
Hilscher Japan KK
Tokyo, 160-0022
Telefon: +81 (0) 3-5362-0521
E-Mail: info@hilscher.jp

Support
Telefon: +81 (0) 3-5362-0521
E-Mail: jp.support@hilscher.com

Korea
Hilscher Korea Inc.
Suwon, Gyeonggi, 443-734
Telefon: +82 (0) 31-695-5515
E-Mail: info@hilscher.kr

Schweiz
Hilscher Swiss GmbH
4500 Solothurn
Telefon: +41 (0) 32 623 6633
E-Mail: info@hilscher.ch

Support
Telefon: +49 (0) 6190 9907-99
E-Mail: ch.support@hilscher.com

USA
Hilscher North America, Inc.
Lisle, IL 60532
Telefon: +1 630-505-5301
E-Mail: info@hilscher.us

Support
Telefon: +1 630-505-5301
E-Mail: us.support@hilscher.com

© Hilscher, 2008-2012